Cour des comptes

QUATRIÈME CHAMBRE **S2025-0602**

PREMIÈRE SECTION

OBSERVATIONS DÉFINITIVES

(Article R. 143-11 du code des juridictions financières)

LA REPONSE DE L'ÉTAT AUX CYBERMENACES SUR LES SYSTEMES D'INFORMATION CIVILS

Le présent document, qui a fait l'objet d'une contradiction avec les destinataires concernés, a été délibéré par la Cour des comptes, le 17 mars 2025

TABLE DES MATIÈRES

SYNTHÈSE

En France, la lutte contre les cybermenaces a été organisée dès 2004 et renforcée significativement après l'attaque informatique massive subie par l'Estonie - à l'encontre des sites gouvernementaux, médias, activités bancaires, etc. -, en avril 2007. Le choix a été fait alors d'un modèle dual de cyberdéfense, fondé sur la séparation des capacités offensives et défensives, modèle peu répandu dans les pays proches.

Une gouvernance spécifique a été mise en place au plus haut sommet de l'État. Elle relève du conseil de défense et de sécurité nationale (CDSN), présidé par le président de la République, réunissant le Premier ministre, les ministres des armées, de l'intérieur, de l'économie, du budget, des affaires étrangères, ainsi que les ministres concernés par les sujets prévus à l'ordre du jour. Ces réunions sont préparées par le comité de direction de la cyberdéfense (CODIR cyber), co-présidé par le chef d'état-major particulier du président de la République (CEMP) et le directeur de cabinet du Premier ministre. Le secrétariat et la mise en œuvre des décisions sont assurés par le secrétariat général de la défense et de la sécurité nationale (SGDSN), rattaché au Premier ministre. Ce positionnement assure une coordination solide entre les sphères de la cyberdéfense et celles de la cybersécurité civile.

Le SGDSN a été doté, de surcroît, d'un opérateur dédié à la cybersécurité – l'agence nationale de la sécurité des systèmes d'information (ANSSI), créée par décret n° 2009-834 du 7 juillet 2009 – qui a développé une expertise reconnue au niveau national comme à l'international.

Alors que la menace a très significativement évolué ces dernières années, la protection des intérêts nationaux est confrontée à un nouveau paradigme qui justifie pleinement la définition, fin 2024, d'une nouvelle stratégie nationale de cybersécurité dont la mise en œuvre doit désormais être déclinée avec les ressources budgétaires afférentes et faire l'objet d'une gouvernance interministérielle renforcée. Ces évolutions nécessitent également de préciser les missions de l'ANSSI et d'accompagner la construction de l'écosystème de cybersécurité en même temps que la diffusion de la culture de la sécurité numérique dans l'ensemble de la société, en rationalisant son financement et les dispositifs de soutien.

Une évolution de la menace qui définit un nouveau paradigme

L'évolution de la menace se caractérise par une croissance continue du nombre et de la sophistication des attaques, une porosité accrue entre l'espionnage et la cybercriminalité, et un élargissement des cibles en direction des maillons faibles des chaînes de production.

Cette mutation est perçue depuis 2015 et la Revue stratégique de cyberdéfense de 2018 a marqué un premier jalon dans la définition d'une politique spécifique de cybersécurité, élargissant son périmètre jusqu'aux entités publiques et économiques les plus fragiles. Jusqu'alors, en effet, les efforts s'étaient concentrés sur la réponse aux incidents et sur la protection des opérateurs d'importance vitale (OIV), publics ou privés, dans le prolongement du dispositif de sécurité des activités d'importance vitale, mis en place en 2006, étendu à la cybersécurité par la loi de programmation militaire pour les années 2014 à 2019 du 18 décembre 2013. Les OIV étaient tenus de veiller à la sécurité de leurs systèmes d'information

d'importance vitale, sous le contrôle et avec l'assistance de l'ANSSI. La directive européenne « *Network and Information System Security* » (NIS 1) de 2016, transposée en droit français en 2018, avait déjà étendu le périmètre des structures concernées et conduit à réguler également les entités qui produisent des services essentiels au bon fonctionnement de la Nation. Le nombre de ces organismes sous contrôle ne dépassait pas cependant 500.

La mutation de la menace, devenue plus diffuse, ne permet plus de s'en tenir à cette démarche, focalisée sur les entités du « *haut du spectre* » particulièrement sensibles pour la défense nationale mais matures en matière de sécurité et dotées de ressources humaines et techniques importantes pour répondre aux menaces par elles-mêmes.

De surcroît, si la France a contribué à la construction d'un dispositif de lutte contre les cybermenaces à l'échelle européenne, elle est en retour assujettie aux dispositions contraignantes voulues par l'Union européenne, notamment dans la directive NIS 2 adoptée le 14 décembre 2022 et qui devait être transposée en droit national au plus tard en octobre 2024. Ainsi, un projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, transposant les trois directives européennes NIS 2 (2022), « Résilience des entités critiques – REC » (2022) et « *Digital Operational Resilience Act* – DORA » (amélioration de la gestion des risques liés aux technologies de l'information et de la communication dans le secteur de la finance, 2022), a été adopté par le Sénat, le 12 mars 2025 ; son adoption définitive par l'Assemblée nationale est attendue d'ici l'été 2025. La nouvelle réglementation élargit très significativement le champ des organismes soumis à des obligations de gestion des risques et d'information en matière de cybersécurité, modulées selon le niveau de criticité des entités, défini par le secteur et leur taille. De l'ordre de 15 000 entités appartenant à 18 secteurs désormais régulés seront ainsi concernées, aussi bien des administrations de toutes tailles que des entreprises allant des PME aux groupes du CAC 40.

Six ans après la publication de la Revue stratégique de cyberdéfense de 2018, la stratégie nationale de cybersécurité, présentée et validée en conseil de défense et de sécurité nationale en novembre 2024, non encore publiée, s'inscrit dans ce nouveau cadre et prend en compte les enseignements de la revue stratégique de 2018. Elle devrait faire évoluer, en la complétant, la gouvernance de la cybersécurité. Sa mise en œuvre doit désormais être déclinée avec les ressources budgétaires afférentes et faire l'objet d'un pilotage interministériel renforcé.

Une réponse aux cyberattaques qui doit s'appuyer plus fortement sur les leviers diplomatiques et judiciaires

La réponse aux cyberattaques est le volet de l'action gouvernementale qui bénéficie de la plus forte antériorité. Elle est pilotée par le SGDSN et s'appuie depuis 2018 sur le « *centre de coordination des crises cyber* » (C4), mécanisme interministériel permanent d'analyse de la menace, de préparation et de coordination de la réponse aux attaques, réunissant les ministères des armées, de l'Europe et des affaires étrangères, de la justice et de l'intérieur, et décliné aux niveaux stratégique et opérationnel. Ce mécanisme gagnerait à mieux prendre en compte les réorganisations opérées au ministère de l'Europe et des affaires étrangères (MEAE) et en matière de traitement de la cybercriminalité.

La constitution, en août 2022, d'une sous-direction de la cybersécurité au sein du MEAE devrait permettre de renforcer la position de la France dans les enceintes diplomatiques destinées à réguler le cyberespace mais également d'accroître la contribution de l'outil

diplomatique français à la réponse aux crises cyber. Il s'agit notamment d'attribuer plus fréquemment ces attaques aux États concernés quand cela est possible et d'utiliser les sanctions prévues par l'Union européenne à l'encontre des personnes ou entités responsables de cyberattaques ou qui apportent un soutien financier, technique ou matériel à des cyberattaques.

La porosité entre espionnage et cybercriminalité nécessite de renforcer les réponses aux cyberattaques criminelles. La réorganisation des forces de sécurité intérieure luttant contre la cybercriminalité, en décembre 2023, est encore trop récente pour que son impact soit évalué. Toutefois, les sujets des redondances et de coordination des structures de gendarmerie et de police constituent encore autant de points de vigilance. En revanche, la structuration d'un pôle spécialisé cyber au sein de la juridiction nationale de lutte contre le crime organisé (JUNALCO) du parquet du tribunal judiciaire de Paris, en 2019, et son renforcement en 2024 ont affiné l'expertise judiciaire et la maîtrise des procédures de poursuite au niveau international. Ce levier pénal mérite d'être mieux articulé avec les services de renseignement, pour éviter toute concurrence dans les enquêtes réalisées. Le fonctionnement du comité judiciaire opérationnel (CJudOps), mis en place officiellement en 2022, après sa préfiguration dès 2020, et son positionnement auprès de l'office anti-cybercriminalité (OFAC) doivent être reconsidérés pour promouvoir un échange d'informations plus performant sur le plan opérationnel. La prise en compte du levier judiciaire fait l'objet de recommandations dans la nouvelle stratégie de 2024 qu'il conviendra de mettre en place rapidement.

Le pilotage interministériel de la cybersécurité à consolider

La Revue stratégique de cyberdéfense publiée en février 2018 soutenait déjà « *une logique de souveraineté numérique dans la profondeur* » intégrant citoyens, entreprises et, pour la première fois, collectivités territoriales. En pratique, la cybersécurité a été progressivement structurée autour de trois volets : outre la réponse de l'État aux agressions, la sécurisation des systèmes d'information de l'État et la protection numérique de la société constituent des axes de l'action gouvernementale. Si la gouvernance d'ensemble s'organise au niveau des services du Premier ministre, le pilotage reste diffus dans les volets autres que celui de la réponse aux cyberattaques.

La sécurisation des systèmes d'information de l'État a connu une accélération significative à l'été 2021. L'instruction générale interministérielle (IGI) n° 1337 a alors structuré l'architecture des responsabilités dans les ministères. Elle entérine, ce faisant, une dichotomie entre stratégie numérique, relevant de la direction interministérielle du numérique (DINUM), service du Premier ministre, placé sous l'autorité du ministre de la Transformation et de la Fonction publiques, et stratégie de sécurité numérique de l'État, rattachée au SGDSN. Le pilotage du dispositif est réalisé en réunions interministérielles (RIM), préparées par un comité stratégique interministériel de la sécurité numérique (COSINUS), présidé par le SGDSN et rassemblant les hauts fonctionnaires de défense et de sécurité (HFDS) de chaque ministère, la directrice interministérielle du numérique et le directeur général de l'ANSSI. Ce dernier préside des comités interministériels de pilotage de la sécurité numérique (CINUS), composés des fonctionnaires de la sécurité des systèmes d'information de chaque ministère. Ce pilotage bien structuré peine cependant à déboucher sur des actions fortes, faute de traduction en plans d'action, appuyés sur des échéanciers précis et articulés avec la programmation budgétaire.

Quant à la protection numérique de la société, outre les réalisations conduites par différents opérateurs en matière d'information, de formation et de qualification des produits, au premier rang desquels figure l'ANSSI, elle fait l'objet d'une « *stratégie nationale d'accélération pour la cybersécurité* » lancée en février 2021 avec le plan de relance post-Covid et, depuis, intégrée dans le plan d'investissement France 2030. Pilotée par le secrétariat général pour l'investissement (SGPI), service du Premier ministre, au travers des opérateurs conventionnés dans ce cadre, cette stratégie vise à développer une politique industrielle de cybersécurité à partir du contrat stratégique de la filière « *industries de sécurité* » établi en janvier 2020. Au-delà de son tropisme en faveur de l'offre plus que des besoins, cette stratégie n'est pas sans conséquence sur la souveraineté nationale. La protection des entreprises et des solutions innovantes relève du dispositif de contrôle des investissements étrangers en France, piloté par la direction générale du Trésor (DGT). À cet égard, si les échanges d'information entre DGT et ANSSI sont réguliers, ils gagneraient à être affinés.

L'hétérogénéité de la gouvernance des trois piliers de cybersécurité plaide pour une plus forte implication du SGDSN dans l'articulation des différentes politiques publiques concourant à la cybersécurité. La nouvelle stratégie de cybersécurité de 2024 confirme le maintien d'un comité directeur cyber, présidé par le Premier ministre et traitant des trois volets de la sécurité numérique pour définir les grandes orientations de l'État en matière de cybersécurité. Elle instaure également un comité de pilotage des politiques publiques cyber (C3PC), à caractère interministériel, sous la responsabilité du SGDSN, chargé d'établir la planification interministérielle pluriannuelle des ressources de l'État, sa déclinaison annuelle et le suivi et la synthèse des moyens dédiés dans les différents ministères. Ces instances apparaissent de nature à renforcer la réponse de la France aux cybermenaces. Leur mise en place devra être rapidement effective.

L'ANSSI : un opérateur d'excellence dont les missions et les moyens doivent être révisés à l'aune de la diffusion des menaces

La sécurisation des systèmes d'information civils français a été incarnée par la création de l'agence nationale de la sécurité des systèmes d'information en 2009. Contrairement à ce que pourrait laisser entendre sa dénomination d'agence, l'ANSSI n'est pas une entité autonome mais un service à compétence nationale, rattaché au secrétariat général de la défense et de la sécurité nationale, auprès du Premier ministre. Il est présent dans tous les volets de la sécurité des systèmes d'information civils : autorité nationale compétente en matière de défense et de sécurité des réseaux et des systèmes d'information, il accompagne les opérations de remédiation des systèmes d'information essentiels victimes de cyberattaques ; il accompagne et contrôle les services de l'État et les opérateurs d'importance vitale (OIV) et de services essentiels (OSE) dans la mise en place d'outils de prévention ; il assure la formation de leurs agents en cybersécurité et la sensibilisation de la population en général aux cybermenaces ; il labellise des solutions de protection ; il est l'expert cyber dans la construction de la réglementation nationale afférente et dans les enceintes internationales.

La croissance de cet organisme, dont le personnel technique est extrêmement qualifié, a été continue depuis sa création. Mais, face à la diffusion de la menace, il s'agit désormais de redéfinir ses moyens d'actions et de les appuyer sur des dispositifs relais. Cette démarche doit orienter la mise en œuvre de ses missions d'assistance aux organismes régulés et de qualification des produits et solutions numériques, de sorte à garantir une offre de biens et

services adaptés aux enjeux des organismes. En matière de réponse aux incidents de sécurité numérique, son action récente en faveur du développement de centres de réponse à incidents numériques (CSIRT) ministériels et régionaux doit déboucher sur une articulation de leurs interventions avec celles des CSIRT sectoriels plus anciens et ses propres réalisations en tant que centre de réponse national (CERT France).

Deux de ses fonctions nécessitent d'être plus particulièrement renforcées : l'observation centralisée et en profondeur de la menace, préalable indispensable à la construction d'une véritable prévention des risques cyber, d'une part ; le contrôle des entités régulées, d'autre part. Cette mission a été jusqu'à présent insuffisamment remplie. Elle doit être structurée pour correspondre à l'élargissement du périmètre des entités assujetties et pour constituer un véritable levier d'amélioration continue de la sécurité des systèmes d'information et de la résilience nationale.

Pour conduire à bien ces évolutions, l'ANSSI doit être dotée d'une feuille de route priorisant ses missions et lui permettant d'ajuster son organisation interne et ses processus de fonctionnement. Le plan stratégique 2025-2027, publié par l'ANSSI en mars 2025, constitue une première étape. Il doit être assorti d'un véritable plan d'actions, d'un échéancier précis et d'une budgétisation des moyens à mettre en œuvre pour atteindre les objectifs visés.

Une intégration de la cybersécurité dans le fonctionnement courant des entités publiques à pérenniser

La sécurisation des entités publiques a jusqu'alors été marquée par de nombreux à-coups. Des mesures de sécurisation des systèmes d'information et de renforcement des capacités de remédiation des ministères ont ainsi été mises en œuvre, à partir notamment de 2021 et sur financement exceptionnel (plan de relance post-Covid), sous l'égide de l'ANSSI, parallèlement à une campagne d'évaluation de la sécurité globale de plusieurs directions d'administration centrale. Il conviendra de s'appuyer sur les constats ainsi réalisés pour dresser des plans d'actions ministériels, assortis d'un échéancier, et d'une programmation budgétaire des ressources à y associer.

L'architecture, notamment organisationnelle de cybersécurité, est comparable entre les services de l'État et les autres opérateurs d'importance vitale ; elle repose en particulier sur le processus d'homologation des systèmes d'information. Cependant, les textes définissant les responsabilités des autorités en matière de sécurité des systèmes d'information au sein des ministères ne leur imposent pas de réaliser les audits subséquents à l'homologation et à son renouvellement ; ils ne prévoient pas non plus de sanctions comparables à ce qui existe pour les organismes régulés. L'articulation entre la feuille de route ministérielle de cybersécurité, prenant en compte les enjeux propres au ministère, et la responsabilisation des autorités qualifiées en sécurité des systèmes d'information (AQSSI) doit être réalisée à travers la formalisation de leurs objectifs dans leur lettre de mission.

La construction d'un écosystème, un accompagnement à mieux structurer

Le plan de relance post-Covid (2020-2022) intégrait la mise en œuvre d'une politique industrielle cyber. Elle a, dans une logique de relance économique par la demande, financé essentiellement l'installation d'outils de sécurisation et les évaluations de la sécurité des systèmes d'information des ministères ainsi que les parcours de cybersécurité des collectivités territoriales et des établissements publics, notamment de santé. Les crédits cyber du plan France 2030 ont quant à eux été dirigés principalement vers des établissements publics de recherche et de formation.

La prise de conscience du besoin de sécurisation des entités locales – collectivités publiques et leurs établissements, petites et moyennes entreprises, etc. – s'est accompagnée de la mise en place d'une profusion de mécanismes et de services d'accompagnement. Si ce foisonnement peut être considéré comme le gage pour chaque utilisateur de trouver des solutions adaptées, il n'en crée pas moins, sur le terrain, une impression de confusion et une illisibilité des dispositifs. De surcroît, plusieurs de ces dispositifs s'appuient sur des crédits étatiques d'amorçage et aucune visibilité n'est donnée sur la pérennisation de leurs ressources. Le modèle économique de ces dispositifs doit donc être repensé et intégré par les organismes disposant des compétences générales de soutien aux collectivités territoriales et aux entreprises.

L'accompagnement de l'écosystème cyber s'est également traduit par différents « outils ». Outre les projets très récents (« 17 Cyber », décembre 2024) ou en cours de finalisation (Cyberscore, filtre anti-arnaque), des dispositifs déjà anciens, comme la plateforme *cybermalveillance.gouv.fr* du groupement d'intérêt public d'assistance aux victimes d'actes de cybermalveillance (GIP Acyma, 2017), ou très récents, comme le Campus cyber (Paris La Défense, 2022), sont encore en recherche d'une définition durable de leurs missions et de leur financement. Il convient désormais de réviser leur modèle économique, en phase avec les besoins du secteur.

Un sujet de ressources humaines à mieux prendre en compte à différents niveaux

La constitution d'une capacité de réponse et de remédiation à des attaques massives et simultanées à l'encontre des intérêts vitaux de la Nation doit privilégier une approche souple et graduée. Si les premières conventions entre le SGDSN et les ministères des armées et de l'intérieur devraient permettre de mobiliser les experts de ces ministères pour renforcer les capacités de l'ANSSI, d'autres pistes méritent d'être étudiées, y compris pour mobiliser en toute sécurité des ressources privées.

L'attractivité des carrières dans la fonction publique reste un sujet sensible, comme dans l'ensemble de la filière numérique publique. Néanmoins, en matière de cybersécurité, il est nécessaire de conjuguer la démarche en sa faveur avec une attention particulière à porter aux conditions de secret des données et à la déontologie des agents, en cas de sortie vers le secteur privé ou des sociétés étrangères.

Enfin, la pénurie de ressources expertes en matière de cybersécurité, partagée par l'ensemble du secteur des technologies de l'information et de la communication, nécessite de

renforcer les plans de formations dispensées aux agents publics mais également, et plus généralement, l'orientation vers les formations initiales et continues dans ces matières.

*

Une nouvelle stratégie nationale de cybersécurité est maintenant finalisée. Elle définit une politique publique globale, visant le développement de l'expertise, le recours à des technologies avancées et le renforcement du pilotage pour répondre aux agressions et conforter la protection des systèmes d'information de l'État et des entités importantes.

Si les objectifs stratégiques sont désormais clairement identifiés, leur traduction dans le secteur public comme la nécessaire acculturation de la société restent à élaborer. Un plan d'actions détaillé, appuyé sur un échéancier précis et une programmation pluriannuelle des ressources, humaines et financières, doit être défini pour garantir l'effectivité d'un processus continu d'amélioration de la cybersécurité et la cohérence du dispositif interministériel mis en place.

RECOMMANDATIONS

Recommandation n° 1 (*SGDSN*) : Adosser la nouvelle stratégie nationale de cybersécurité de 2024 sur un échéancier précis des actions à mener et sur une programmation pluriannuelle des ressources, humaines et financières, à mettre en œuvre dans la sphère des services de l'État.

Recommandation n° 2 (*SGDSN, ministère de la justice, ministère de l'intérieur*) : En matière de lutte contre la cybercriminalité, renforcer la coordination entre les autorités judiciaires et les services de renseignement.

Recommandation n° 3 (*SGDSN, ANSSI*) : Définir l'articulation entre les CSIRT ministériels, sectoriels et territoriaux et s'assurer de la pérennité de leur financement.

Recommandation n° 4 (*SGDSN, ANSSI*) : Mettre en place à court terme un observatoire de la cybermenace au sein de l'ANSSI, centralisant à l'échelle nationale les données et les analyses, afin d'en prévoir l'évolution et les moyens de la prévenir et de la contrer.

Recommandation n° 5 (*SGDSN, ANSSI*) : Établir une cartographie des risques à partir des résultats des mesures d'accompagnement et d'audits réalisés ; intensifier et prioriser les contrôles réalisés par l'ANSSI et les entités de contrôle sectorielles.

Recommandation n° 6 (*SGDSN, ANSSI*) : Définir une programmation pluriannuelle des moyens de l'ANSSI cohérente avec la nouvelle stratégie nationale de cybersécurité et le plan stratégique 2025 de l'Agence.

Recommandation n° 7 (SGDSN) : Renforcer la sensibilisation des dirigeants des services de l'État aux enjeux des cybermenaces et leur fixer des objectifs précis en la matière dans leur lettre de mission.

Recommandation n° 8 (*SGDSN, ANSSI*) : Conformément à l'IGI 1337, établir des conventions entre le SGDSN, l'ANSSI et chaque ministère, fixant les objectifs pluriannuels à atteindre en matière de cybersécurité, un échéancier d'actions et les moyens à mettre en œuvre.

Recommandation n° 9 (*SGDSN*) : Proposer un modèle économique pérenne de fonctionnement pour le GIP Acyma et le Campus cyber.

Recommandation n° 10 (*SGDSN, ANSSI*) : Établir des critères de labélisation des solutions de cybersécurité répondant aux besoins des petites et moyennes entreprises et collectivités territoriales.

Recommandation n° 11 (*SGDSN, ANSSI*) : Adapter l'offre interne de formation aux besoins des organismes régulés et développer la fonction d'observation et d'orientation de l'offre de formation en cybersécurité.

INTRODUCTION

L'évolution des cybermenaces - c'est-à-dire du risque d'attaque des systèmes informatiques - est intimement liée à l'essor des technologies de l'information et de la communication. Des premiers virus informatiques des années 1970 aux cyberattaques[1] d'aujourd'hui, potentiellement sophistiquées et massives, la cybersécurité – entendue comme l'état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace[2] - s'est imposée comme un enjeu majeur pour les individus, les entreprises et les gouvernements.

En France, dès 2008, le Livre blanc sur la défense et la sécurité nationale identifie les attaques contre les systèmes d'information comme l'une des principales menaces qui pèsent sur la défense et la sécurité[3] de la Nation. Pour y répondre, l'agence nationale de la sécurité des systèmes d'information (ANSSI)[4] a été créée en 2009. Contrairement à ce que son appellation laisse entendre, il ne s'agit pas d'un organisme indépendant mais d'un service à compétence nationale, rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), organisme interministériel placé sous l'autorité du Premier ministre. Ce positionnement stratégique souligne à la fois le niveau élevé de prise en compte de la menace mais également la nécessité de son traitement multisectoriel et interministériel.

Parallèlement le ministère des armées bénéficie d'une organisation spécifique : le commandement de la cyberdéfense (COMCYBER), créé en mai 2017[5] et placé sous l'autorité directe du chef d'état-major des armées (CEMA), rassemble l'ensemble des forces de cyberdéfense du ministère des armées. À ce titre, il conduit des opérations militaires dans le cyberespace avec des actions de lutte informatique offensive (LIO) et de lutte informationnelle et d'influence (L2I) et assure également la sécurité numérique, en mettant en place l'ensemble des techniques et pratiques visant à protéger les systèmes informatiques, les réseaux et les données contre les attaques ou accès non autorisés, garantissant ainsi l'intégrité, la confidentialité et la disponibilité des informations numériques, du ministère des armées.

---

[1] Cf. glossaire de l'ANSSI : Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

[2] Cf. glossaire de l'ANSSI : Espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet.

[3] « *(…) blocage malveillant, destruction matérielle, neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles (…)* ».

[4] Décret n°2009-834 du 7 juillet 2009 portant création de l'agence nationale de la sécurité des systèmes d'information, en tant que service à compétence nationale (SCN), rattaché au secrétaire général de la défense et de la sécurité nationale.

[5] Décret n° 2017-743 du 4 mai 2017 relatif aux attributions du chef d'état-major des armées et l'arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées.

La création de l'opérateur des systèmes d'information interministériels classifiés (OSIIC)[6] en 2020, ainsi que celle du service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)[7], en 2021, tous deux érigés en services à compétence nationale et rattachés au SGDSN, a renforcé la spécialisation de l'ANSSI en cybersécurité civile.

Le présent rapport se concentre sur le périmètre de la cybersécurité civile, déjà vaste puisqu'il concerne l'ensemble des acteurs de la Nation, englobe différents leviers - juridiques, techniques, industriels, et de gestion des ressources humaines - et recouvre des actions intérieures, au niveau national et dans les territoires, mais également des prises de position à l'échelle européenne et internationale. Il ne traite ni des domaines militaires, ni des actions relevant de l'OSIIC et de Viginum.

Dans le champ de la cybersécurité civile, face à la prolifération des cyberattaques, l'État a révisé sa stratégie nationale de cybersécurité en cohérence avec l'évolution du cadre réglementaire européen (1ère partie) et fait évoluer la gouvernance d'ensemble dans un mouvement qui devra être conforté (2ème partie). Ces évolutions nécessitent de préciser les missions de l'ANSSI (3ème partie) et d'accompagner le renforcement de l'écosystème cyber ainsi que la diffusion de la culture de la sécurité numérique dans l'ensemble de la société, en rationalisant son financement et les dispositifs de soutien (4ème partie).

[6] Par le décret n° 2020-455 du 21 avril 2020. Il résulte de la fusion entre l'ex sous-direction du numérique (SDN) de l'ANSSI, chargée de proposer, concevoir et mettre en œuvre des produits et des systèmes d'information sécurisés au profit des ministères, des opérateurs d'importance vitale et de l'ANSSI elle-même, d'une part, et le Centre de transmissions gouvernemental (CTG) chargé de protéger les communications gouvernementales, d'autre part.

[7] Décret n° 2021-922 du 13 juillet 2021.

1 Face aux enjeux actuels des cybermenaces, une nouvelle stratégie nationale de cybersécurité à mettre en œuvre

Les cybermenaces croissent au rythme de l'évolution rapide des technologies numériques et du contexte international. Pour les contrer, l'Union européenne a renforcé son dispositif juridique et la France a fait évoluer sa stratégie, dont la nouvelle version date de la fin de 2024.

1.1 Des cybermenaces croissantes et de plus en plus sophistiquées

La croissance continue des attaques, l'élargissement des cibles visées et la vulnérabilité des activités étatiques à la cybercriminalité, sont des tendances lourdes, relevées dès le rapport de l'Assemblée nationale sur la cyberdéfense en 2018[8].

1.1.1 Une croissance continue et diversifiée des attaques

Le niveau de la menace cyber a continué de croître en 2023-2024, dans un contexte marqué par de nouvelles tensions géopolitiques, au Proche-Orient notamment, et la tenue d'évènements internationaux sur le sol français (Coupe du monde de rugby 2023 et Jeux olympiques et paralympiques 2024).

L'Agence de l'Union européenne pour la cybersécurité (ENISA[9]), dans son panorama des menaces 2023[10], relève une augmentation significative des cyberattaques qui lui sont signalées, aussi bien en volume qu'en nature et en impact.

Au niveau national, l'ANSSI en fait également le constat dans son évaluation de la cybermenace en 2023 comme en 2024[11].

L'observation des attaques visant des entités moins sensibles, réalisée à travers les sollicitations adressées à la plateforme *cybermalveillance.gouv.fr*, gérée par le Groupement d'Intérêt Public d'assistance aux victimes d'actes de cybermalveillance (GIP ACYMA)[12], fait aussi apparaître une augmentation du nombre d'attaques et leur diversification.

[8] Rapport d'information de l'Assemblée nationale N° 1141, du 4 juillet 2018, relatif à la cyberdéfense.
[9] Acronyme en anglais pour *European Union Agency for Cybersecurity*
[10] ENISA Threat Lanscape 2023, July 2022-June 2023.
[11] Panorama de la cybermenace 2024, version du 11 mars 2025, réf. CERTFR-2025-CTI-003.
[12] Créé par arrêté du 3 mars 2017, le GIP Acyma est porté par un partenariat public privé, son conseil d'administration regroupant l'ANSSI, et plusieurs ministères - chargés de l'économie, de l'intérieur, de la justice, des armées et le ministère de l'éducation nationale – et des acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs. En 2024, le groupement d'intérêt public est fort de 65 membres.

Tableau n° 1 : Les trois principales cybermenaces recensées par la plateforme cybermalveillance.gouv.fr en 2023

Catégorie de publics	Hameçonnage		Piratage de compte		Fraudes* / Rançongiciel	
	2023	Variation en volume /2022	2023	Variation en volume /2022	2023	Variation en volume /2022
Particuliers *	38 %	- 6 %	17,1 %	+ 22 %	2,9 % 2,3 % 3,8 %	+ 87 % + 93 % + 78 %
Entreprises et associations	21,2 %	+ 2 %	23,5 %	+ 26 %	16,6 %	+ 8 %
Collectivités et administrations	26,9 %	+ 26 %	17,5 %	+ 22 %	21 %	+ 36 %

* Les fraudes concernent les particuliers et les chiffres présentés correspondent à la fraude à la carte bancaire, au vol et usurpation d'identité et au faux conseiller bancaire.

Source : Cour des comptes, d'après le rapport d'activité du GIP Acyma 2023.

Le commandement dans le cyberespace du ministère de l'intérieur (COMCYBER-MI) confirme ces tendances, dans son premier rapport annuel sur la cybercriminalité publié le 30 juillet 2024[13]. Ainsi**,** 278 703 infractions liées au numérique ont été enregistrées par les forces de sécurité intérieures en 2023, en augmentation de 9 % par rapport à 2022. Selon les statistiques du ministère de l'intérieur[14], 59 % de ces infractions sont des atteintes « numériques » aux biens (escroqueries, arnaques en ligne etc.), 34 % des atteintes « numériques » à la personne et 5 % des atteintes aux institutions.

L'ENISA relève que les rançongiciels[15] figurent en tête des événements portés à sa connaissance, avec un volume de 34,1 %, suivis par les attaques par déni de service - DDoS[16] (28,2 %) et contre les données (17,2 %).

1.1.2 Un élargissement significatif des cibles et secteurs visés

Si les rançongiciels restent bien en 2023 l'activité cybercriminelle prédominante, même si aucune attaque significative affectant des « entités » de l'Union européenne n'a été relevée, le centre de veille, d'alerte et de réponse à incidents sur les systèmes d'information de l'Union

[13] https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024
[14] Référence : service statistique ministériel de la sécurité intérieure (SSMSI).
[15] Un rançongiciel est un logiciel malveillant qui chiffre les données et les systèmes d'une victime pour les rendre inaccessibles. L'attaquant demande ensuite une rançon, généralement en cryptomonnaie, en échange de la clé de déchiffrement qui permettra de rétablir l'accès.
[16] *Distributed Denial of Service* (déni de service distribué) : Les attaques par déni de service (DoS) et celles par déni de service distribuées (DDoS) sont des tentatives malveillantes de rendre un serveur, un service ou une ressource réseau indisponibles pour leurs utilisateurs. L'origine d'une attaque DoS est unique, alors qu'une attaque DDoS est lancée à partir de plusieurs sources, et parfois distribuée de manière globale.

européenne (CERT-UE)[17] identifie que les intentions des cyberattaquants sont en tout premier lieu, le cyberespionnage (73 %) loin devant « l'hacktivisme » (16 %), la cybercriminalité (7 %) et les opérations de désinformation/mésinformation (4 %)[18]. De ce fait, les cibles visées par les attaques ne sont plus réservées à des organismes ou des secteurs sensibles mais concernent un nombre croissant de victimes potentielles.

L'analyse établie par l'ENISA en 2023 – qui porte sur le secteur civil - montre qu'au niveau européen, les administrations publiques sont les secteurs les plus ciblés par les cyberattaques (cf. tableau ci-dessous). Elles représentent 19 % des évènements observés, les positionnant loin devant les attaques contre les particuliers (11 %), les établissements de santé (8 %) et les entreprises de la filière des infrastructures numériques (7 %).

Tableau n° 2 : Principales natures des menaces observées par secteurs sur la période juillet 2022-juin 2023

Natures des attaques	Principaux secteurs touchés
Rançongiciels	Industrie (14 %) Santé (13 %) Administration publique (11 %) Services publics (9 %)
DDoS	Administration publique (34 %) Transport (17 %) Banques/Finances (9 %)
Vols de données	Administration publique (16 %) Santé (10 %) Particuliers (15 %)

Source : Cour des comptes, avec les données ENISA Threat Landscape 2023

Dans son analyse des événements cyber dans les 25 secteurs qu'il surveille au niveau de Union européenne, le CERT-UE relève que, pour l'année 2023[19], en dehors du secteur de l'administration publique fortement attaqué, 13 secteurs ont subi au moins 10 cyberattaques, avec en tête la diplomatie, la défense, le transport, la finance, la santé, l'énergie, le secteur « technologie »[20].

Au niveau national, l'ANSSI fait le constat d'une multiplicité croissante des entités et des outils attaqués, dans son panorama de la cybermenace 2023, confirmé en 2024. Elle souligne le maintien d'un espionnage stratégique et industriel, avec une forte augmentation du ciblage d'entités travaillant dans des domaines stratégiques – groupes de réflexion, instituts de recherche et base industrielle et technologique de défense (BITD[21]) – ou qui assurent la

[17] CERT-UE (Computer Emergency Response Team), disposant d'équipes d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE.
[18] CERT-UE, Threat Landscape Report 2023 – Year review, V1.1 – February 2024.
[19] *Idem* note n°14.
[20] Auxquels s'ajoutent la justice, les télécommunications, la recherche, l'éducation, les droits fondamentaux et l'espace.
[21] La BITD regroupe l'ensemble des entreprises de défense contribuant à concevoir et à produire les équipements pour les armées

transmission de données sensibles, comme les entreprises de télécommunications et de fourniture de services numériques. Elle constate une modification des outils ciblés et l'augmentation du nombre d'attaques contre des téléphones portables professionnels et personnels afin d'espionner des individus cibles, une évolution des cibles attaquées et un contournement des mesures de cyberdéfense mises en place par les opérateurs sensibles, par l'agression d'entités moins armées, appartenant à leur chaîne d'approvisionnement (Supply Chain) : partenaires, sous-traitants, prestataires ou organisations de tutelle. Enfin, elle note, en 2023, un regain du nombre d'attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation. Ce type d'attaques à but de déstabilisation menées par des groupes *hacktivistes* se confirme en 2024.

1.1.3 Une « industrialisation » des cybermenaces

Tous les « observateurs » de la menace cyber relèvent, en 2023, une amélioration des capacités offensives des cyberattaquants via une internationalisation des cybermenaces et une professionnalisation significative de la cybercriminalité, que ce soit en matière d'appropriation des outils techniques ou de structuration en véritables réseaux.

Cette tendance est notamment soutenue par la prolifération de solutions logicielles offensives commercialisées par des entreprises privées, comme des outils de vol d'informations (*infostealers*). La fuite de générateurs et de codes sources de rançongiciels comme LockBit, Babuk ainsi que Conti en 2021 et 2022, puis le démantèlement de Qakbot en août 2023, ont permis leur appropriation par des acteurs moins expérimentés qui génèrent puis déploient leurs propres rançongiciels. Des guides d'intrusion cyber sont désormais vendus ou diffusés sur des forums cybercriminels.

Le cas de la porte modulaire *DarkCrystal Rat*

En 2018, la porte modulaire DarkCrystal Rat est mise en vente sur des forums russophones. Elle est composée d'un *stealer* (programme malveillant qui collecte différents types d'informations tels que les identifiants, les mots de passe, les jetons d'authentification avant de les transmettre à son opérateur), d'une interface de commande et d'un outil d'administration. Sa structure modulaire permet de l'adapter aux objectifs de l'attaquant en ajoutant des modules d'enregistrement de frappe, de collectes d'identifiants ou encore des captures d'écran.

Le faible prix de cet outil (4 500 roubles pour un abonnement de deux mois, soit une cinquantaine d'euros) et sa disponibilité en source ouverte en ont rapidement fait un outil populaire auprès de plusieurs acteurs cybercriminels. Selon le CERT-UA (service d'intervention d'urgence ukrainien), il a été utilisé pour compromettre des organisations ukrainiennes des secteurs des médias et des télécommunications.

Les méthodes employées par les acteurs cybercriminels ont également connu des évolutions notables qui compliquent le traitement de cette menace. C'est le cas par exemple du rançonnage reposant exclusivement sur l'exfiltration de données (sans déploiement de rançongiciel), observée depuis 2021, et déployé en 2023 dans le cadre de campagnes d'attaques massives.

En outre, les cybercriminels s'engagent dans la commercialisation du « cyber-crime-as-a-service » (CaaS), brouillant ainsi les pistes de l'identification des attaquants et de leurs motivations.

1.2 Un cadre européen de plus en plus prescriptif

Face aux évolutions de cybermenaces désormais omniprésentes, la France a développé des stratégies de cybersécurité, en s'inscrivant dans un cadre européen de plus en plus élaboré.

1.2.1 Une régulation européenne de cybersécurité civile élargie et plus précise

Si la France affiche une ambition souveraine en matière de cyberrésilience, elle la développe dans un cadre européen, de plus en plus dense depuis 2016.

1.2.1.1 Une construction progressive de la cybersécurité européenne

L'un des actes fondateurs de régulation du cyberespace émane du Conseil de l'Europe avec l'adoption le 8 novembre 2001 de la Convention de Budapest sur la cybercriminalité[22]. Entrée en vigueur en 2004, la convention de Budapest a largement dépassé le cadre européen. Elle est devenue un traité international, ratifié par 76 États parties, dont les États-Unis. La Fédération de Russie est le seul État membre du Conseil de l'Europe à ne pas avoir signé la convention.

Cette convention a anticipé l'amplification de la cybercriminalité. Elle a pour ambition d'harmoniser et de renforcer les législations nationales en matière d'incrimination et de sanctions pénales comme d'investigation et de preuve. Elle sert de base à la coopération internationale entre les parties à la convention et prévoit les conditions d'assistance réciproque des parties, dans le cas – fréquent – d'incriminations transnationales.

La convention de Budapest a fait, à partir de septembre 2017, l'objet d'importantes négociations visant à la doter d'un deuxième protocole additionnel, adopté le 12 mai 2022, mais non encore entré en vigueur. Il permet le renforcement de la coopération et de la divulgation de preuves électroniques.

Parallèlement au Conseil de l'Europe, l'Union européenne est très active sur la cybersécurité et s'est dotée d'un certain nombre d'outils dédiés.

Elle a notamment créé très rapidement, dès 2004, une agence chargée de la sécurité des réseaux et de l'information (ENISA)[23], dont le siège est en Grèce. Elle constitue un centre d'expertise pour la cybersécurité en Europe afin d'assister les pouvoirs publics dans l'identification des enjeux et de proposer des solutions techniques pour lutter contre les menaces. Ses missions principales sont de conseiller les institutions de l'UE et les États membres en matière de cybersécurité et de favoriser l'échange de bonnes pratiques, en mettant notamment en place des partenariats entre le secteur public et le secteur privé, en particulier les

[22] https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/090000168008156d
https://rm.coe.int/16800ccea4
https://eur-lex.europa.eu/FR/legal-content/summary/convention-on-cybercrime.html

[23] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'agence européenne chargée de la sécurité des réseaux et de l'information.

entreprises spécialisées dans ce domaine. L'ENISA organise depuis 2010 un exercice bisannuel dénommé *Cyber Europe*, qui permet aux États membres de tester leur collaboration en cas de crise.

Très récemment, le règlement européen « E-Evidence »[24] a simplifié l'accès aux données électroniques détenues par les fournisseurs de service pour faciliter la lutte contre la cybercriminalité au sein de l'UE. Il entrera en vigueur en 2026[25].

Depuis 2016, l'Union européenne a également défini une réglementation de plus en plus précise en matière de protection des systèmes d'information civils.

Le premier champ couvert a été celui de la protection des données. Le règlement général sur la protection des données (RGPD) de l'Union européenne de 2016[26] renforce et unifie les mécanismes nationaux en la matière et établit un régime de responsabilité pour les gestionnaires de ces données. Sa particularité est de pouvoir s'appliquer, en Europe, à des acteurs extra-européens.

Autre axe de réglementation, la sécurité des réseaux et des systèmes d'information fait l'objet de nombreuses directives et règlements qui définissent progressivement des normes de plus en plus élevées pour renforcer la cyberrésilience des membres.

Entrée en vigueur dans le droit européen le 6 juillet 2016, la directive européenne sur la sécurité des réseaux et des systèmes d'information de 2016, dite « directive NIS » (*Network and Information Systems Security* (UE) 2016-1148) a été transposée en 2018 en droit français[27]. Elle vise à renforcer la réactivité des 27 États membres face aux cybermenaces, à augmenter collectivement le niveau de protection en renforçant la sécurité des opérateurs jugés essentiels au bon fonctionnement de la société. Elle comporte également des obligations en direction des fournisseurs de services numériques (FSN) [28].

---

[24] Règlement E-Evidence 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023, relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de peines privatives de liberté prononcées à l'issue d'une procédure pénale.

[25] Sa mise en œuvre soulève des enjeux juridiques, stratégiques et opérationnels. En particulier, la future « autorité compétente » française qui sera chargée d'examiner les notifications des injonctions de production de preuves électroniques (trafic et contenu) - au moment de la rédaction du présent rapport, un groupe de travail était réuni pour préparer cette décision - devra s'assurer que les demandes qui lui seront adressées ne contreviennent pas aux intérêts des enquêtes menées sur le territoire national.

[26] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[27] Loi n° 2018-133 du 26 février 2018, portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ; décret n° 2018-384 du 23 mai 2018 ; arrêté du 13 juin 2018 portant sur les modalités de déclaration des incidents ; arrêté du 1er août 2018 relatif au coût des contrôles par l'ANSSI ; arrêté du 29 septembre 2018 relatif aux règles de sécurité des OSE et leurs délais d'application.

[28] Est considéré comme FSN et soumis à des obligations tout opérateur fournissant des places de marché en ligne, qui permettent à des consommateurs ou à des professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels ; les moteurs de recherche en ligne ; les services d'informatique en nuage. Tout FSN implanté ou fournissant son service à l'intérieur de l'UE doit appliquer les dispositions prises pour la transposition de la directive NIS sitôt que l'une des conditions suivantes est atteinte : son nombre d'employés est supérieur ou égal à 50 ; son chiffre d'affaires annuel est supérieur à 10 millions d'euros.

1.2.1.2 De nouvelles directives face à l'amplification des menaces

Adoptée en novembre 2022, la directive NIS 2 (UE) 2022-2555 est entrée en vigueur dans le droit européen le 14 décembre 2022, avec l'objectif pour les États membres de la transposer dans leur droit national au plus tard le 17 octobre 2024.

Cette directive NIS 2 renforce les mesures de protection à mettre en œuvre face aux cybermenaces et élargit significativement le périmètre des organismes soumis à régulation. En effet, les entités concernées par NIS 2 répondent à trois critères cumulatifs : une activité fournie ou exercée au sein de l'UE ; le secteur d'activité[29], leur taille[30]. Les administrations publiques (centrales et régionales) et les infrastructures numériques fournissant certains services (services DNS, registres de nom de domaine de premier niveau, services de confiance qualifiés, réseaux de communications électroniques publics, services de communications électroniques publics, services de communications électroniques accessibles au public) sont assujetties à la réglementation, quelle que soit leur taille.

Plus prescriptive que la directive NIS 1, elle définit des mesures de gestion des risques en matière de cybersécurité et des obligations d'information non seulement pour les entités essentielles mais également pour les entités importantes, distinguées selon leur niveau de criticité[31], défini par le secteur et la taille. Les normes elles-mêmes sont modulées selon l'appartenance des entités à l'une ou l'autre des catégories.

Elle met en place un régime de sanctions administratives[32], opposables aux entités dont la pratique contreviendrait à ces normes.

Enfin, elle amène les États membres à renforcer leur coopération en matière de gestion de crise cyber, en donnant notamment un cadre formel au réseau CyCLONe (*Cyber Crisis Liaison Organisation Network*) qui rassemble l'ANSSI et ses homologues européens.

D'autres réglementations récentes visent la cybersécurité en l'incluant dans un cadre plus vaste de protection, comme la directive européenne 2022-2557 sur la résilience des entités

[29] Le texte européen liste en annexe tous les secteurs pour lesquels la directive s'appliquera. L'annexe 1 définit les onze "secteurs hautement critiques" : énergie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène) ; transport (aériens ferroviaires, par eau, routiers) ; secteur bancaire ; infrastructure des marchés financiers ; santé ; eau potable ; eaux usées ; infrastructure numérique ; gestion des services TIC (interentreprises) ; administration publique ; espace. L'annexe 2 définit les sept "autres secteurs critiques" : services postaux et d'expédition ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et distribution des denrées alimentaires ; fabrication ; fournisseurs numériques ; recherche.

[30] Sont assujetties les moyennes ou grandes entreprises au sens de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises. Une moyenne entreprise vérifie au moins un des deux points suivants : au moins 50 travailleurs à temps plein ; au moins 10 millions d'euros de chiffre d'affaires annuel total.

[31] Définies grossièrement, les entités essentielles (EE) sont les grandes entreprises au sens de la recommandation du 6 mai du 2003 (plus de 250 salariés et/ou plus de 50 millions de chiffre d'affaires) qui font partie des "secteurs hautement critiques" ainsi que les deux cas particuliers des infrastructures numériques et des administrations publiques ; les entités importantes (EI) sont les moyennes entreprises au sens de la recommandation du 6 mai 2003 qui font partie des "secteurs hautement critiques" ainsi que les moyennes et grandes entreprises qui font partie des "autres secteurs critiques".

[32] Les États peuvent instaurer également des sanctions pénales, selon le principe du *non bis in idem*.

critiques (REC), ou en se focalisant sur un secteur d'activité, comme la directive DORA[33], (*Digital Operational Resilience Act*) et le règlement associé, qui prescrivent un certain nombre de mesures pour améliorer la gestion des risques liés aux technologies de l'information et de la communication (TIC), dans le secteur de la finance. Adoptées fin 2022, elles doivent être transposée par les États membres dans leur droit national à des échéances comparables à celles de la directive NIS 2, soit, respectivement, octobre 2024 et janvier 2025.

L'Union européenne a également produit deux règlements majeurs, d'application directe, très récemment :

- le Cybersecurity Act, en vigueur depuis le 27 juin 2019, établit des normes de cybersécurité pour l'Union Européenne, avec un cadre législatif obligatoire pour les États et volontaire pour les entreprises. Il vise à sécuriser les produits, services et processus dès leur conception, en introduisant un système de certification avec trois niveaux d'assurance : élémentaire, substantiel et élevé, pour rendre le marché de la cybersécurité plus lisible, permettant aux consommateurs de faire des choix éclairés et contribuant à un marché numérique unique ;
- tout récemment, le Cyber Solidarity Act, adopté en décembre 2024, et entré en vigueur le 4 février 2025, vise à renforcer la coopération transnationale en matière de cybersécurité au sein de l'UE. Il met en place une infrastructure paneuropéenne composée de centres d'opérations de sécurité[34], dans le but d'améliorer les capacités communes de détection et d'appréciation de la situation, et un mécanisme d'urgence afin d'aider les États membres à se préparer et à réagir aux incidents de cybersécurité importants et majeurs, et à s'en rétablir immédiatement. Le soutien à la réaction aux incidents est également mis à la disposition des institutions, organes et organismes de l'Union. Il établit une réserve de cybersécurité de l'Union, sous la responsabilité de la Commission européenne, composée de services de réaction aux incidents fournis par des fournisseurs privés, de confiance. Les utilisateurs des services de la réserve de cybersécurité de l'Union comprennent les autorités des États membres chargées de la gestion des crises de cybersécurité et les CSIRT ainsi que les institutions, organes et organismes de l'Union.

1.2.2 La transposition des directives dans la législation française : entre aménagements et bouleversements

1.2.2.1 Une interaction fructueuse entre législation nationale et réglementation européenne

En France, le Livre blanc de la défense et de la sécurité de 2013 étendait aux opérateurs d'importance vitale (OIV) l'exigence de cybersécurité. La loi de programmation militaire pour

[33] La directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 a pour objectif de modifier les directives existantes, notamment Solvabilité 2, afin de les mettre en cohérence avec les nouvelles dispositions du règlement DORA.
[34] *Security Operation Center* (SOC).

les années 2014 à 2019[35] a donc introduit des mesures de sécurité obligatoires pour les OIV afin de protéger les infrastructures critiques, qu'elles soient publiques ou privées contre les cyberattaques.

Ces mesures s'inscrivaient dans le prolongement des règles de sécurité déjà définies pour les installations d'importance vitale, définies dès l'ordonnance n° 58-1371 du 29 décembre 1958 tendant à renforcer la protection de ces installations, essentiellement par des normes bâtimentaires. En 2006, le dispositif de sécurité des activités d'importance vitale est mis en place pour associer les OIV, publics ou privés, à la mise en œuvre de la stratégie de sécurité nationale en termes de protection contre les actes de malveillance (terrorisme, sabotage) et les risques naturels, technologiques et sanitaires. La cybersécurité est donc intégrée dans un cadre juridique spécifique, comme un des volets de la sécurité des OIV.

Les OIV sont ainsi tenus de veiller à la sécurité de leurs systèmes d'information d'importance vitale (SIIV), ceux pour lesquels « *l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population* ». Pour chaque secteur d'activité concerné, un arrêté du Premier ministre précise les critères permettant aux opérateurs d'identifier les systèmes d'information soumis à ce nouveau dispositif, les règles de sécurité informatique qui s'y appliqueront et les modalités de déclaration des incidents les affectant. Ces arrêtés ont été publiés entre 2016 et 2020[36].

Les premiers organismes soumis à des règles de sécurité numérique sont des entités matures sur le plan de la sécurité et de taille suffisante pour abriter en interne les ressources nécessaires à leur mise en œuvre, avec le soutien et sous le contrôle de l'ANSSI.

Ce cadre normatif français, précurseur au sein de l'UE, a orienté la directive européenne NIS 1 de 2016, transposée en France par la loi de 2018. Toutefois, cette directive a étendu le périmètre des entités soumises à des obligations de cybersécurité, aux fournisseurs de service numérique (FSN), mais également aux « *opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services* ».

Le choix a été fait, en France, de maintenir le dispositif des OIV et de définir une nouvelle catégorie d'opérateurs, les opérateurs de services essentiel (OSE), pour se conformer à la norme européenne. Les OSE sont désignés par arrêté du Premier ministre, sur proposition des ministres compétents dans les secteurs mentionnés en annexe du décret de 2018[37].

---

[35] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

[36] Les OIV sont désignés par le ministre coordonnateur du secteur. La liste recouvre plus de 200 opérateurs, publics ou privés, et elle est couverte par le secret de la défense nationale. Les dates de publication diffèrent selon les secteurs : produits de santé, gestion de l'eau, alimentation, approvisionnement en énergie électrique, gaz naturel, hydrocarbures pétroliers, transport terrestre, transport maritime et fluvial et transport aérien (1er octobre 2016) ; audiovisuel et information, communications électroniques et Internet, industrie et finances (1er janvier 2017) ; nucléaire (1er avril 2017) ; activités industrielles de l'armement et espace (1er octobre 2017) ; activités civiles de l'État (1er octobre 2019) ; recherche publique (1er octobre 2020).

[37] Énergie, transport, logistique, banques, infrastructures des marchés financiers, services financiers, assurance, social, emploi et formation professionnelle, santé, fourniture et distribution d'eau potable, traitement des eaux non potables, infrastructures numériques, éducation, restauration.

La loi de 2018 définit donc un cadre juridique spécifique[38] qui rejoint les principes de base posés par la loi de programmation militaire à l'intention des OIV, sans être identique :

- les OSE comme les OIV doivent identifier en leur sein un interlocuteur privilégié de l'ANSSI ;
- ils doivent définir et tenir à jour la liste de leurs systèmes d'information essentiels (SIE), comme les OIV le font avec les systèmes d'information d'importance vitale (SIIV). Cette cartographie doit prendre en compte les services rendus par les prestataires de l'entreprise ;
- comme les OIV, les OSE doivent notifier directement à l'ANSSI des incidents affectant leurs systèmes d'information ;
- ils ont l'obligation de se soumettre aux règles de sécurité édictées par le Premier ministre (SGDSN / ANSSI)[39]. Elles ne sont pas totalement identiques mais très comparables et concernent les thématiques suivantes : gouvernance et pilotage de la sécurité informatique, maîtrise des risques, maîtrise des systèmes d'information, gestion des incidents de sécurité, protection des systèmes d'information ;
- ils ont, enfin, l'obligation de se soumettre à des contrôles afin d'évaluer leur niveau de sécurité. Le contrôle est conduit par l'ANSSI, par un autre service de l'État ou par un prestataire d'audit qualifié par l'ANSSI pour les OIV ; par l'ANSSI ou un prestataire d'audit de sécurité des systèmes d'information (PASSI) pour les OSE. Les contrôles sont à la charge des opérateurs. Les arrêtés du 23 mars et du 1er août 2018 fixent le coût d'un contrôle effectué par l'ANSSI à 1200 € nets la journée.

Quelques points distinguent cependant les deux régimes, avec un niveau d'exigence plus élevé à l'égard des OIV :

- les OIV doivent recourir obligatoirement à des produits et des services qualifiés par l'ANSSI ;
- seuls les OIV ont l'obligation de déployer des « systèmes de détection » qualifiés par l'ANSSI (permettant l'identification des marqueurs techniques de cyberattaque, *i.e.* sondes). Ces dispositifs sont opérés soit par l'ANSSI directement, soit par un prestataire de détection d'incident de sécurité (PDIS) agréé par l'ANSSI, ce qui permet à l'ANSSI d'avoir une vision assez précise des éventuelles menaces pesant sur les SI concernés ;
- le Premier ministre peut imposer des mesures aux OIV afin de répondre à une crise majeure menaçant ou affectant la sécurité des systèmes d'information.

[38] Complété par le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique et l'arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

[39] Dans le décret n°2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale ou dans l'arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

1.2.2.2 Un nécessaire « passage à l'échelle » avec le renforcement des mesures de cybersécurité au niveau européen

L'ANSSI et, notamment, sa sous-direction de la stratégie, mène le travail de transposition de la directive NIS 2, conjointement avec le SGDSN qui conduit celle de la directive REC et la direction générale du travail en charge de la directive DORA, dans un souci bienvenu de simplification, conduisant à fondre dans un seul et même projet de loi nommé « Résilience » les exigences de ces trois textes pour rendre plus facile leur application[40].

La méthode choisie décline la réglementation européenne sur trois niveaux, législatif, réglementaire et infra-réglementaire. Pour ce dernier niveau, le parti a été pris de le faire reposer sur une diffusion de guides et la définition de moyens techniques acceptables de conformité emportant présomption de conformité. Cette démarche semble effectivement propice à la lisibilité du dispositif.

Le projet de loi, relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, n° 1112 a été présenté en conseil des ministres le 15 octobre 2024 et déposé au Parlement le même jour. La dissolution de l'Assemblée nationale a retardé l'adoption du projet. Après engagement de la procédure accélérée, il a été adopté par le Sénat le 12 mars 2025 et déposé à l'Assemblée nationale, le jeudi 13 mars 2025.

Les dispositions de la directive NIS 2 étendent significativement le champ des entités concernées. En France, cela se traduit par une augmentation du nombre de secteurs régulés de 7 à 18 secteurs[41]. La directive élargit également le périmètre des systèmes d'information à sécuriser dans chaque organisme, jusqu'alors réduit aux systèmes d'information essentiels. Avec NIS 2, les obligations s'appliquent par défaut à l'ensemble des systèmes d'information de l'entité[42].

L'application de la directive entraînera une augmentation du nombre d'entités régulées que l'ANSSI estime de 500 à 15 000 entités environ. Ce décompte reste imprécis. En effet, alors que les organismes soumis à NIS 1 étaient désignés par l'autorité nationale compétente, avec NIS 2, il leur appartient désormais de s'identifier. Outre le travail avec les organisations professionnelles des secteurs concernés et des actions élargies de communication, l'ANSSI met à disposition l'espace numérique « Mon Espace NIS 2 » qui permet aux entités de déterminer si elles relèvent ou non de la règlementation. Ce portail doit leur permettre également de s'enregistrer en ligne. L'incertitude devra être levée rapidement car la directive prévoit que la liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine doit être établie par les États membres, au plus tard le 17 avril 2025.

---

[40] Un travail de simplification sur les règlementations nationales en matière de cybersécurité est également conduit au niveau de l'ANSSI dans le cadre du projet de loi « Résilience ».

[41] La directive européenne NIS 1 couvrait six secteurs : eaux potables, énergie, finances, infrastructures numériques, santé, transports. Lors de sa transposition au niveau français ont été introduits les secteurs suivants : assurance, eaux non potables, éducation, emploi, logistique, restauration, social. NIS 2 élargit le cadre d'application à de nouveaux secteurs : services TIC (interentreprises), administration publique de l'État et du territoire, espace, services postaux et d'expédition, gestion des déchets, fabrication (dont produits chimiques), recherche, fournisseurs numériques, agroalimentaire.

[42] Des mécanismes d'exemption de certains systèmes d'information seront toutefois permis si ces derniers n'affectent pas la réalisation des activités ou la fourniture des services de l'entité.

Alors que la directive NIS 2 laisse libre choix aux États membres de soumettre ou non les collectivités territoriales aux nouvelles règles, la France a décidé de les intégrer dans ces nouvelles exigences, au regard de la multiplication des attaques affectant les services publics locaux et leur faible sécurisation.

L'intégration des collectivités territoriales dans la règlementation

Les attaques informatiques affectant les collectivités territoriales sont nombreuses : de janvier 2022 à juin 2023, l'ANSSI a traité 187 incidents concernant les collectivités territoriales, soit 17 % de l'ensemble des incidents traités par l'agence sur la période. Leurs conséquences peuvent affecter de multiples champs de compétences et de nombreux citoyens.

La décision de les intégrer dans le périmètre des entités régulées est assortie d'une approche proportionnée, adaptée aux moyens et à la maturité des acteurs.

- 661 collectivités territoriales ou groupements de collectivités territoriales devraient être concernés au titre des entités essentielles : les régions de métropole ainsi que les régions et pays et territoires d'outre-mer (22 entités) ; les départements de métropole et d'outre-mer (97 entités) ; les métropoles, communautés urbaines et communautés d'agglomération de métropole et d'outre-mer (263 entités) ; les communes de plus de 30 000 habitants de métropole et d'outre-mer (279 entités).
- Les 992 communautés de communes de métropole et d'outre-mer seront quant à elles concernées au titre des entités importantes.
- La très grande majorité des communes (99 % ont moins de 30 000 habitants) ne sont donc concernées que par leur intercommunalité de rattachement.

Les exigences de sécurité imposées par NIS 2 sont proportionnées selon que les entités sont définies comme essentielles, les plus sensibles, ou importantes. La première catégorie recouvre, de facto, les organismes déjà régulés en France et l'essentiel des exigences les concernant sont déjà prises en compte. Les entités de la seconde catégorie, la plus importante en nombre, sont soumises à des exigences allégées, conçues pour diminuer leur probabilité d'être atteintes par un rançongiciel courant, sans nécessiter des investissements disproportionnés. Il s'agit, en effet, d'éviter tout risque de « surtransposition » de la directive, sujet qui fait cependant l'objet de débats vifs devant les assemblées parlementaires, concernant notamment les contraintes imposées aux collectivités locales, PME et organismes de recherches. Un amendement sénatorial fait ainsi basculer de la catégorie « d'entité essentielle » vers celle d'« entité importante », les communautés d'agglomération ne comprenant pas au moins une commune de plus 30 000 habitants.

Pour prévenir les inquiétudes sur les coûts induits par les mesures de protection, le SGDSN a chiffré de manière approximative, dans les délais qui lui étaient imposés, les coûts induits par l'application des nouvelles règles :

- pour les entités essentielles qui sont souvent des organismes bien dotés en ressources financières et humaines – notamment dans le secteur privé –, l'effort estimé est limité car l'investissement a déjà été réalisé pour appliquer les normes existantes : les coûts d'investissements sont évalués entre 450 000 à 880 000 euros, avec un coût annuel de maintien en condition de sécurité s'élevant environ à 10 % du coût d'investissement ;
- pour les entités importantes, les normes imposées par NIS 2 relèvent principalement de règles élémentaires et de la mise en place de routines d'« hygiène » en cybersécurité : les coûts d'investissement sont évalués entre 100 000 et 200 000 euros, avec un coût annuel de maintien en condition de sécurité s'élevant à environ 10% du coût d'investissement.

Les coûts d'investissement comme les dépenses de maintenance restent somme toute modestes, en tous cas, « absorbables » dans des budgets ministériels ou d'organismes publics et privés. Du reste, les travaux d'un cabinet d'étude spécialisé dans l'analyse de la sécurité numérique des organismes[43] faisait état d'une part de 5,5 %[44] du budget numérique consacré à la cybersécurité, dans les grands groupes privés, et d'un ratio moyen d'ETP cyber correspondant à un ETP pour 1199 agents.

Il convient, de surcroît, de mettre en perspective les investissements nécessaires pour respecter les obligations NIS 2 avec le coût constaté d'une cyberattaque. En effet, quelle que soit l'ampleur de la cyberattaque, le montant des investissements qu'une entité doit mobiliser pour se sécuriser est inférieur aux coûts réels d'une attaque et de ses conséquences.

Des coûts de sécurisation inférieurs aux coûts moyens d'une cyberattaque

(Source : ANSSI)

Dans la sphère publique, les établissements hospitaliers ont supporté des dégâts particulièrement importants. Les coûts directs ont été estimés à 2,36 M€ pour le centre hospitalier Dax-Côte d'Argent (février 2021) et à plus de 5,5 M€ pour le centre hospitalier Sud-Francilien de Corbeil-Essonnes (août 2022). Les collectivités territoriales et les intercommunalités ont également été lourdement affectées, avec des coûts directs estimés à 960 000 euros pour la Métropole Aix-Marseille-Provence (mars 2020) et à plus de 1,5 M€ pour la ville de Bondy (novembre 2020)[45]. À ces coûts directs s'ajoutent des coûts indirects, liés aux activités non réalisées ou à la perte de confiance des usagers, mais leur chiffrage est complexe, tout particulièrement dans le cas de missions de service public.

Dans la sphère privée, une enquête menée en juin 2024 par l'ANSSI auprès des membres du CLUSIF, une association de professionnels de la cybersécurité, révèle qu'une cyberattaque coûte en moyenne 466 000 euros pour les TPE/PME, 13 millions d'euros pour les ETI et 135 M€ pour les plus grandes entreprises. Ce coût représente en moyenne 5 à 10% du chiffre d'affaires de l'organisation, quels que soient sa taille ou son secteur d'activité, réparti entre les pertes d'exploitation (50%), le coût des prestations externes d'accompagnement (20%), le coût de remise en état et d'investissement dans le système d'information (20%) et le coût réputationnel (10%). Ce coût des cyberattaques reste largement sous-évalué, certains opérateurs reconnaissant ne pas prendre en compte tous les coûts systématiquement, voire reconnaissant que certains coûts restent impossibles à quantifier.

Les mesures obligatoires à mettre en œuvre par les entités concernées seront assorties de sanctions[46], dans un délai qui reste à fixer au plan national, car la directive européenne ne prévoit pas les délais de mise en œuvre. Sans que le projet de loi ne puisse l'intégrer, il est aujourd'hui envisagé un délai de trois ans après la publication des textes réglementaires pour la mise en conformité relative aux objectifs de sécurité[47]. Alors même que NIS 2 permettait la

[43] Wavestone

[44] Cette moyenne ne tient pas compte des investissements passés ni de la répartition entre investissement et fonctionnement.

[45] Les exemples retenus pour estimer les coûts de ces cyberattaques sont ceux qui ont fait l'objet de communications publiques de la part des victimes.

[46] Les contrôles pourront donc donner lieu à des injonctions, voire à des sanctions administratives potentiellement très élevées en cas de manquement (jusqu'à 2 % du chiffre d'affaires pour les entités essentielles et 1,4 % pour les entités importantes), en complément des sanctions pénales déjà existantes, via une commission des contrôles indépendante qui devra être en mesure de statuer, et dont la composition et les compétences restent à définir.

[47] Pour les obligations d'enregistrement auprès de l'autorité nationale et de communication d'informations (article 12 du projet de loi) ainsi que de notification d'incidents (article 17 du projet de loi), le délai envisagé est plus court : les entités devraient mettre en œuvre ces obligations au plus tard six mois après la publication des décrets

mise en place de sanctions pénales et administratives, il convient de noter que le choix a été fait, lors de la transposition en droit français, de ne définir que des sanctions administratives, dans un souci de modération.

La mise en œuvre de la directive NIS 2 bouscule donc l'écosystème français, aussi bien public que privé.

1.3 Une nouvelle stratégie nationale de cybersécurité à mettre en œuvre

De nombreux documents stratégiques ont été établis depuis 2008. Tout d'abord inscrite dans le cadre de la cyberdéfense, la cybersécurité[48] a progressivement bénéficié de documents dédiés. Cette émancipation résulte pour partie de la prise en compte des mutations des menaces et des évolutions des règles européennes.

1.3.1 Une stratégie initialement marquée par la cyberdéfense

1.3.1.1 Une orientation vers les entités les plus critiques

Le sujet de la cybersécurité a été appréhendé originellement au travers de la cyberdéfense et des lois de programmation militaire, ce qui explique la focalisation sur la sécurisation des systèmes d'information des entités critiques. Il est identifié dès le Livre blanc sur la défense et la sécurité nationale de 2008 et traité à nouveau par celui de 2013. Cette inscription dans la stratégie de défense a conduit naturellement à penser la cybersécurité dans le cadre de réflexion des armées. C'est ainsi que les premières mesures de sécurisation ont été édictées dans la loi de programmation militaire de 2013 et visent plus particulièrement les opérateurs d'importance vitale.

Identifiant la cyberdéfense comme un axe essentiel de la défense nationale, la stratégie de 2013 a fait l'objet d'une révision en 2017. Elle réaffirme l'importance de la cyberdéfense et appelle à « *la préservation de la capacité de la France à agir de manière souveraine dans le cyberespace* ». Cette ambition est confortée en 2021 par le ministère des armées dans le document intitulé « Actualisation stratégique 2021 ».

d'application. En effet, ces obligations requièrent uniquement la mise en place de mesures organisationnelles ou techniques mineures avec de faibles coûts associé.

[48] Selon le glossaire établi par les assises de la cybersécurité (https://www.lesassisesdelacybersecurite.com/fr-FR/glossaire-cyber/cybersecurite-et-cyberdefense), « *La sécurité est un état recherché tandis que la défense est une posture* ». Outre cette différence, il est considéré que « *la cybersécurité couvre le domaine de la protection des systèmes d'information de manière générale (technologies, organisations, processus, lois…), tandis que la cyberdéfense décrit plutôt ce qui est du ressort de la défense nationale (« l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels* ») ».

1.3.1.2 L'émergence de stratégies dédiées à la cybersécurité

En parallèle de ces travaux, une *« stratégie nationale de défense et de sécurité des systèmes d'information »*[49] a été élaborée en 2010 par le SGDSN et soumise à l'approbation du Premier ministre en application du 7° de l'article R*1132-3 du code de la défense. À partir de cette date, des stratégies dédiées à la cybersécurité sont régulièrement établies pour décliner les orientations de la défense nationale.

Après la parution du Livre blanc sur la défense et la sécurité nationale de 2013 et la loi de programmation militaire de 2014-2019, une « *stratégie nationale pour la sécurité du numérique* » a été élaborée et publiée en 2015. Elle se décline en cinq objectifs stratégiques[50] qui prennent déjà en compte, outre la sécurité numérique de l'État et des infrastructures critiques, la cybercriminalité, la formation, l'Europe. En écho à l'association de la base industrielle et technologique de défense (BITD) dans la stratégie de défense, la stratégie de sécurité numérique promeut la conduite d'une politique industrielle.

La Revue stratégique de cyberdéfense (RSC) publiée en février 2018, en lien avec la loi de 2018 de transposition de NIS 1, est une somme très complète d'analyses, d'orientations et de mesures à mettre en œuvre pour faire de l'État le « *responsable de la cyberdéfense de la Nation* ». Elle repose sur la défense d'« *une logique de souveraineté numérique dans la profondeur* » intégrant citoyens, entreprises et, pour la première fois, collectivités territoriales. Ce faisant, elle s'inscrit, malgré son titre, dans une logique englobante de défense et de sécurité du numérique, en cohérence avec la stratégie de 2015. À rebours de son appellation, ce document ne se contente pas de faire un état des lieux des acteurs et de la menace ni de décrire le modèle français de cyberdéfense, mais il définit des actions précises[51], y compris dans les domaines de la lutte contre la cybercriminalité[52] et à l'international, la mise en place de mesures différenciées[53] pour l'État et les OIV, d'une part, les OSE, d'autre part.

Le document conforte la séparation entre capacités défensives et offensives, propre au modèle français. En effet, celui-ci est considéré comme plus respectueux des libertés individuelles et de la protection de la vie privée et permettant « *le développement de relations de confiance entre des acteurs privés et les services de l'État chargés de la cyberprotection* ».

Le document comporte une liste de 18 recommandations prioritaires, à mettre en œuvre dans l'immédiat ou dans un court et moyen terme pour « *une ambition* [française] *de cyberdéfense renforcée* ». Ces recommandations sont déclinées en 50 mesures. Elles ont, pour

---

[49] https://www.sgdsn.gouv.fr/nos-missions/proteger/assurer-la-cybersecurite-et-coordonner-la-cyberdefense#haut-de-page

[50] Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure ; confiance numérique, vie privée, données personnelles, cybermalveillance ; sensibilisation, formations initiales, formations continues ; environnement des entreprises du numérique, politique industrielle, export et internationalisation ; Europe, souveraineté numérique, stabilité du cyberespace.

[51] En matière de formation, la RSC recommande l'éducation en cybersécurité, pour tous, et de renforcer les formations spécialisées, notamment auprès des femmes. Le sujet de l'attractivité des carrières publiques est également traité.

[52] Pour faire face à la cybercriminalité, la RSC 2018 engage à évaluer plus finement les actes malveillants, à renforcer l'efficacité de la réponse judiciaire, à rapprocher les acteurs de la lutte contre la cybercriminalité et ceux de la cyberdéfense, et à développer un réseau international de collaboration entre magistrats et enquêteurs.

[53] Utilisation généralisée de sondes pour les systèmes d'information de l'État, renforcement de la sécurité des opérateurs super critiques et développement d'une offre privée labellisée pour les OIV, application des règles de NIS 1 pour les opérateurs de service essentiel, offre de solutions labellisées pour les collectivités territoriales.

la plupart, guidé l'action, à l'international, dans les ministères et les collectivités territoriales et dans le soutien à l'offre de solutions et au tissu industriel (cf. *infra*).

Pour autant, alors qu'un suivi des recommandations par des rapports semestriels d'avancement et de mise en œuvre du SGDSN, transmis au comité de pilotage cyber, était prévu, l'examen des comptes rendus des réunions du centre de coordination des crises cyber (C4) n'a pas fait apparaître de suivi de ces recommandations durant les exercices récents.

1.3.2 Une nécessaire adaptation aux nouvelles menaces et au cadre européen

Le contexte en matière de cybersécurité a effectivement fortement évolué depuis 2018, avec notamment une menace qui s'accroît au niveau stratégique en affectant les cibles les plus critiques avec un haut degré de sophistication et une menace cybercriminelle dont l'ampleur pose des problèmes de sécurité nationale. De fait, le dispositif national de cyberdéfense a été continuellement adapté pour prendre en compte toutes ces évolutions.

Cependant, la Revue nationale stratégique (RNS) de 2022, qui affiche une nouvelle ambition nationale pour le domaine cyber (voir encadré *infra*), et la mise en œuvre de la nouvelle réglementation européenne (NIS 2, REC, DORA) engagent à définir une nouvelle stratégie nationale de cybersécurité.

La Revue nationale stratégique de 2022 : vers une résilience cyber de premier rang

Lancée en juillet 2022 et présentée par le Président de la République le 9 novembre 2022 à Toulon, la Revue nationale stratégique de 2022 promeut l'objectif stratégique n°4 qui vise « *une résilience cyber de premier rang* » et en précise les contours : « *disposer de capacités adaptées et organisées, permettant de prévenir ou, le cas échéant, de réduire l'impact et la durée des cyberattaques menées à l'encontre de la France, a minima pour les fonctions les plus critiques*. »

Cet objectif stratégique se décline en trois priorités : 1/ améliorer la résilience cyber de la France, condition de la souveraineté ; 2/ consolider les acquis du modèle français ; 3/ investir dans la durée pour atteindre le meilleur niveau de résilience cyber. Les orientations données mobilisent non seulement le ministère de la Défense mais également les entreprises relevant de la BITD.

Ainsi, face à l'évolution rapide de la menace, une nouvelle revue stratégique de cyberdéfense a été demandée par le président de la République en octobre 2023, avec trois objectifs : « *tirer les leçons de la Revue stratégique de cyberdéfense [de 2018], en s'appuyant notamment sur les initiatives d'amélioration continue ; bâtir la RSC 2024 sur l'analyse de l'évolution de la menace cyber, en couvrant les nouvelles gammes de risques et les progrès - actuels et attendus - de la technologie ; proposer un rebond stratégique de l'organisation de cyberdéfense, en évaluant notamment le besoin de transformation des politiques publiques impactées et les modalités de mise en œuvre* ». Le mandat a été confié à l'adjoint numérique et cyber du délégué général pour l'armement (DGA) du ministère des armées, avec le soutien du SGDSN qui a assuré le secrétariat des travaux.

Les conclusions de cette revue stratégique de cyberdéfense se sont traduites par un document, intitulé *« stratégie nationale de cybersécurité* » qui s'inscrit dans le nouveau cadre décrit *supra* et prend en compte les enseignements de la revue stratégique de 2018.

La mise en œuvre de cette nouvelle stratégie devrait s'appuyer, par ailleurs, sur un renforcement de la gouvernance actuelle (voir *infra*) au niveau interministériel.

Présentée et validée en fin d'année 2024, elle n'a pas encore fait l'objet d'une publication officielle, ni d'une déclinaison publique sous forme de plan d'action et de financements dédiés.

Comme le soulignent les objectifs fixés à l'exercice 2024 et l'absence de suivi de la RSC 2018, la cadence de la parution de tels textes – tous les 5 à 6 ans – illustre moins l'adaptation de la France à l'évolution des menaces que la nécessité de relancer régulièrement la politique de lutte contre les cyberattaques, faute d'assurer la continuité de l'action au niveau national.

Ce point doit être un sujet d'attention dans le pilotage de la mise en œuvre de cette nouvelle stratégie. Pour garantir la réalisation des actions préconisées, il apparaît nécessaire de décliner la stratégie nationale de cybersécurité en plan d'action interministériel, précisant les responsabilités des acteurs publics mais également les interactions à mettre en place avec les acteurs privés ainsi que les ressources affectées.

Recommandation n° 1. (*SGDSN*) Adosser la nouvelle stratégie nationale de cybersécurité de 2024 sur un échéancier précis des actions à mener et sur une programmation pluriannuelle des ressources, humaines et financières, à mettre en œuvre dans la sphère des services de l'État.

CONCLUSION INTERMEDIAIRE

L'évolution des cybermenaces qui présentent désormais un caractère hybride - entre espionnage et cybercriminalité – et diffus – touchant tous les secteurs d'activité et l'ensemble des organismes de la chaîne de production -, rend nécessaire la régulation d'un nombre plus important d'entités, dans le but de les prémunir plus efficacement contre les attaques numériques. Le renforcement de la réglementation en matière de cybersécurité, opéré dans une interaction fructueuse entre les niveaux européen et national, définit un nouveau cadre de fonctionnement pour l'ensemble de la société.

Si la France s'est dotée dès les années 2000 d'une stratégie de sécurisation numérique de ses entités critiques pour le bon fonctionnement de la société, le saut quantitatif et qualitatif, dicté par l'état de la menace et l'évolution de la réglementation, a conduit à définir une nouvelle stratégie nationale de cybersécurité fin 2024. Les orientations établies emportent des conséquences importantes, tant sur la gouvernance du dispositif de sécurisation que sur le fonctionnement de l'opérateur central et des ministères et l'accompagnement de l'écosystème. Elles appellent la mise en place d'un échéancier précis des actions à mener et une programmation pluriannuelle des ressources à mettre en œuvre pour atteindre les objectifs visés.

2 UNE GOUVERNANCE A RENFORCER

Sous l'impulsion des stratégies successives, la gouvernance de la cybersécurité s'est adaptée aux mutations des menaces. Ces évolutions doivent être confortées.

2.1 Un positionnement interministériel de la gouvernance stratégique de la cybersécurité à conforter

2.1.1 Une responsabilité confiée au plus haut niveau de l'État

La sécurité des systèmes d'information est inscrite dans le code de la défense (art. L.2321-1 à L.2323-6). La responsabilité en est explicitement portée, depuis la LPM n°2013-1168 du 18 décembre 2013, par le Premier ministre. Celui-ci « *définit la politique et coordonne l'action gouvernementale* » mais il le fait « *dans le cadre de la stratégie de sécurité nationale et de la politique de défense* » qui relève du président de la République.

En pratique, la stratégie est donc décidée par ce dernier, via le conseil de défense et de sécurité nationale (CDSN), qui réunit sous sa présidence, en formation plénière, le Premier ministre, les ministres des armées, de l'intérieur, de l'économie, du budget, des affaires étrangères, ainsi que les ministres concernés par les sujets prévus à l'ordre du jour. Un conseil de défense et de sécurité nationale dédié à la cybersécurité est organisé une fois par an[54].

La revue stratégique de cyberdéfense de 2018 instaure un comité de direction de la cyberdéfense (dit comité directeur cyber - CODIR cyber), co-présidé par le chef d'état-major particulier du président de la République (CEMP) et le directeur de cabinet du Premier ministre, qui prépare et suit les décisions prises en CDSN. Les membres permanents du CODIR cyber sont les cabinets du ministère de l'intérieur et du ministère des armées, ainsi que les représentants des directions et services directement impliqués dans le domaine de la cyberdéfense. Les directeurs de cabinet des ministères de l'Europe et des affaires étrangères, de la justice et de la ministre déléguée chargée de l'intelligence artificielle et du numérique peuvent y être invités en fonction des sujet inscrits à l'ordre du jour.

Les secrétariats des CDSN et du CODIR cyber sont assurés par le SGDSN. Placé auprès du Premier ministre, le SGDSN incarne institutionnellement le continuum entre sécurité intérieure et sécurité extérieure, acté depuis le Livre blanc sur la défense et la sécurité nationale de 2008[55].

---

[54] La cyberdéfense est traitée dans le fonctionnement courant des CDSN, sans avoir été érigée en Conseils particuliers – contrairement aux Conseils de défense écologique ou aux Conseils de défense sanitaire – ni en formations spécialisées, contrairement au Conseil national du renseignement ou au Conseil de l'armement nucléaire.

[55] Amorcé avec la création du Conseil supérieur de la défense nationale (CSDN), le 4 avril 1906, cet organisme prit d'abord la forme d'un simple secrétariat non permanent, avant de devenir tour à tour secrétariat général puis état-major, et finalement secrétariat général de la défense nationale à partir de 1962. Depuis 2009, l'ajout du terme

2.1.2 Un caractère interministériel à renforcer

Conçue en contrepoint de la cyberdéfense, la cybersécurité s'applique sur un périmètre ministériel incomplet, avec le positionnement spécifique du ministère des armées, responsable du volet de lutte informatique offensive mais également de la sécurité de ses propres systèmes d'information et des relations avec la BITD - dont la direction générale de l'armement (DGA) du ministère est le pivot. Cette partition rend cruciaux le partage des données et des analyses, la convergence de l'action et une coordination permanente.

Des pays optant pour une forte proximité entre services à vocation offensive ou défensive

Plusieurs pays n'opèrent pas de distinction nette entre les entités en charge des volets offensif et défensif.

C'est le cas au Royaume-Uni : si deux entités distinctes prennent en charge ces deux volets (le National Cyber Security Centre – NCSC, créé en 2016 et la National Cyber Force – NCF – créée en 2020), elles sont toutes les deux liées aux services de renseignement. Le NCSC est en effet rattaché au Government Communications Headquarters (GCHQ), tandis que la NCF a été créée en s'appuyant essentiellement sur le GCHQ et le ministère de la défense.

Cette intégration ou cette grande proximité des volets défensif et offensif se retrouve dans d'autres pays comme les Pays-Bas (Algemeine Inlichtigen en Veiligheidsdiens - AIVD), la Corée du sud (National Intelligence Service) et la Norvège (la Nasjonal Sikkerhetsmyndghet, intégrée au ministère de la défense).

Cette coordination est à l'œuvre en France et la nouvelle stratégie nationale de cybersécurité considère que « *la gouvernance mise en place permet de garantir une très forte coordination entre les pôles défensif et offensif* ».

Face à la diffusion des cybermenaces à tous les niveaux de la société, une structuration de la politique de cybersécurité a été réalisée, à partir de 2018, en trois volets : l'organisation de la réponse de l'État aux cyberattaques, le pilotage de la cybersécurité de l'État et de ses établissements publics, et la coordination des politiques publiques visant à renforcer la cybersécurité de l'ensemble du tissu social.

Chacun de ces volets dispose d'une gouvernance propre (cf. *infra*). Si l'ensemble de ces structures est rattaché peu ou prou aux services du Premier ministre, le niveau de contrôle est néanmoins diversifié, très direct pour la réponse aux cyberattaques mais relativement distant pour la protection des systèmes d'information des entités du « bas du spectre ». L'implication du SGDSN dans ces différents axes d'action est également variable : s'il est particulièrement présent dans la réponse aux agressions, il l'est moins dans la gestion de la sécurisation des ministères où son pilotage procède essentiellement de son expertise cyber. Ce constat est encore plus avéré dans le déploiement des politiques publiques visant à accompagner l'émergence d'un écosystème de cybersécurité. Cet état de fait éclaire la difficulté rencontrée par le SGDSN pour répondre à la demande de la Première ministre, en janvier 2023, de s'assurer « *de la cohérence d'ensemble et de la complémentarité des capacités d'action de l'État* » en matière de cybersécurité, en identifiant « *les éventuelles redondances entre les financements réalisés et/ou programmés par les ministères, ou absences de financement sur des segments critiques* ». Le recensement des crédits affectés aux ministères, dans le cadre de la mise en œuvre des différents plans d'action et feuilles de route en cours à cette date, n'a permis qu'une compilation de

« sécurité » à son nom a marqué l'élargissement de ses compétences dans ce domaine, conformément aux orientations du Livre blanc sur la défense et la sécurité nationale de 2008.

chiffres hétéroclites, établis sur une base déclarative, mélangeant des périodes différentes, pour certaines échues (comme pour les 176 M€ du plan France Relance qui couvrait les exercices 2020 à 2022), pour d'autres à échéance lointaine (comme le plan France 2030) et embrassant un périmètre très large, comprenant les crédits des ministères de l'intérieur, de la santé et des armées, pour la partie défensive de son action, et, notamment, ceux destinés à sécuriser ses propres systèmes d'information.

Cet exercice démontre l'absence de visibilité globale et de suivi de la politique publique de cybersécurité. La nouvelle stratégie nationale de cybersécurité de 2024 préconise le maintien effectif d'un « *comité directeur cyber* », présidé par le Premier ministre, réunissant au minimum une fois par an les cabinets ministériels concernés, et couvrant l'ensemble des trois volets de la sécurité numérique pour définir les grandes orientations de l'État en matière de cybersécurité et suivre la mise en œuvre des décisions prises en CDSN. Le secrétariat de ce comité revient au SGDSN. Il apparaît, en effet, nécessaire d'articuler plus fortement les actions au niveau interministériel.

2.2 Un renforcement des structures ministérielles à mieux prendre en compte dans la réponse aux agressions

La Revue nationale de cyberdéfense de 2018 a défini un mécanisme interministériel permanent d'analyse de la menace, de préparation et de coordination, associant l'ensemble des ministres concernés et l'a dénommé « centre de coordination des crises cyber » (C4). Alors que la revue prévoyait trois niveaux de C4 – stratégique, technique et restreint permanent et technique -, la coordination ne s'est opérée qu'à deux niveaux : stratégique (C4 Strat) et technique (C4 TechOps).

Présidé par le SGDSN, le C4 Strat réunit mensuellement les acteurs principaux de la cybersécurité - ministères des armées, de l'Europe et des affaires étrangères, de la justice et de l'intérieur -, afin de faire le point sur l'état de la menace cyber et de définir puis proposer aux autorités les stratégies de réponse adaptées.

Le C4 TechOps, organisé sous la forme d'une cellule permanente depuis les arbitrages du conseil de défense et de sécurité nationale dédié au cyber de juin 2021, permet la coordination et la conduite des travaux opérationnels entre l'ANSSI, le commandement de la cyberdéfense (COMCYBER – état-major des armées), la direction générale de l'armement, la direction générale de la sécurité intérieure (DGSI), et la direction générale de la sécurité extérieure (DGSE). Cette enceinte autorise le partage de connaissances sur les menaces stratégiques, avérées ou potentielles, à l'encontre des intérêts nationaux, le traitement conjoint des incidents d'ampleur qui visent les intérêts français et la mutualisation de certaines capacités.

2.2.1 Une dimension internationale des cybermenaces désormais mieux prise en compte par le ministère de l'Europe et des affaires étrangères

Pour renforcer la dimension internationale de la réponse aux cybermenaces, une sous-direction de la cybersécurité a été créée en août 2022 au sein de la direction des affaires stratégiques, de sécurité et du désarmement de la direction générale des affaires politiques et de

sécurité du ministère de l'Europe et des affaires étrangères. Cette sous-direction contribue à la définition et à la mise en œuvre de la politique étrangère de la France dans le domaine de la cybersécurité et de la lutte contre la cybercriminalité. À ce titre, elle participe, au sein du C4 Strat, à l'élaboration des stratégies de réponse aux cyber-attaques visant les intérêts de la France et de ses alliés. L'équipe demeure néanmoins restreinte puisque cette sous-direction abrite, fin 2024, seulement un sous-directeur, son adjointe et quatre rédacteurs.

Une feuille de route, assortie d'un plan d'action détaillé, lui a été assignée le 13 février 2023. Elle mentionne quatre objectifs stratégiques : contribuer par l'action diplomatique dans les cadres collectifs de l'UE et de l'OTAN au renforcement de la posture de défense et de résilience française dans le cyberespace ; développer une culture de solidarité via le renforcement capacitaire (à froid) et l'assistance cyber (à chaud) au profit des alliés et partenaires ; consolider un cadre normatif assurant la stabilité et la sécurité du cyberespace, en lien avec l'ambassadeur pour le numérique, notamment via l'établissement d'un programme d'action de l'ONU dédié à l'horizon 2025 ; accroître la contribution de l'outil diplomatique français à l'analyse de la menace, la prévention et la réponse aux crises cyber.

Dans cette perspective, la France, conjointement avec le Royaume-Uni, a récemment lancé un processus diplomatique visant à élaborer des options de régulation et d'action pour lutter contre la prolifération et l'usage irresponsable des capacités de cyber-intrusion (ex. : logiciels espions) disponibles sur le marché. Un centre de compétences cyber dans les Balkans occidentaux, monté en partenariat entre la France, le Monténégro et la Slovénie, a été inauguré le 9 décembre 2024 à Podgorica. Proposant des formations et des outils pour lutter contre la cybercriminalité, il vise à renforcer les compétences en cybersécurité dans la région, à améliorer la cyber-résilience des pays des Balkans occidentaux et par ressaut, celle des membres de l'Alliance atlantique et candidats à l'adhésion à l'Union européenne.

La réalisation de ces objectifs nécessite une coordination renforcée avec les pays affinitaires, en particulier pour le partage de renseignements, mais également au niveau du C4 Strat. Le but est, en effet, de mieux mobiliser les instruments diplomatiques disponibles en réponse aux attaques informatiques, notamment les sanctions à l'échelle européenne.

Sanctions à l'échelle européenne

En mai 2019, le Conseil de l'Union européenne (UE) a établi un cadre de sanctions qui vise des personnes ou entités responsables de cyberattaques ou de tentatives de cyberattaques, qui apportent un soutien financier, technique ou matériel à des cyberattaques ou qui sont impliquées de toute autre manière dans de telles attaques. Des sanctions peuvent également être imposées à d'autres personnes ou entités qui leur sont associées.

Ce régime de sanctions couvre les cyberattaques qui ont une incidence significative et qui ont leur origine ou sont menées à l'extérieur de l'UE, qui utilisent des infrastructures situées en dehors de l'UE, sont menées par des personnes ou entités établies ou opérant en dehors de l'UE ou sont menées avec le soutien de personnes ou d'entités opérant en dehors de l'UE.

Les mesures restrictives, qui comprennent, à l'encontre des personnes, l'interdiction de voyager vers l'UE et, à l'encontre des personnes et entités, le gel des avoirs, ont été prorogées en dernier lieu jusqu'au 18 mai 2025.

En juillet 2020, ce régime de sanctions a été utilisé pour la première fois, en imposant une interdiction de pénétrer sur le territoire de l'UE et un gel des avoirs à l'encontre de six personnes – deux de nationalité chinoise, quatre appartenant au renseignement militaire russe - ainsi qu'un gel des avoirs à l'encontre de trois entités ou organismes – une branche des forces armées russes, deux entités chinoises. Ces personnes et entités ont participé à des cyberattaques visant des entreprises établies dans l'UE, telles que les cyberattaques connues sous le nom de WannaCry, NotPetya ou Operation Cloud Hopper, ou à la tentative de cyberattaque contre l'Organisation pour l'interdiction des armes chimiques (OIAC).

L'attribution des attaques à un État fait partie de l'arsenal des mesures de rétorsion. En effet, si l'attribution est techniquement complexifiée par l'évolution de la menace et l'intrication entre États et groupes privés cybercriminels, et politiquement délicate au regard des enjeux stratégiques internationaux du pays victime, la « réputation » est une donnée essentielle dans le cyberespace et la démonstration de capacités techniques importantes de l'État victime, conjuguée à la perte de crédibilité de l'agresseur, constitue un moyen de dissuasion très efficace. Pour autant, la France, contrairement aux États-Unis et au Royaume-Uni[56], reste prudente sur l'attribution à un État en matière de cyberattaque. La manœuvre la plus aboutie à ce jour consiste en l'imputation d'une cyberattaque, par le directeur général de l'ANSSI, le 21 juillet 2021, à un groupe APT31, sans citer le pays qui lui est affilié[57]. La structuration du ministère de l'Europe et des affaires étrangères pourrait permettre un recours plus intensif à l'attribution des menaces.

Attribution par l'UE de l'attaque KA-SAT

Cette attaque menée dans la nuit du 23 au 24 février 2022 ne ciblait pas le satellite en lui-même, mais les équipements au sol qui dépendaient de lui. Ainsi, plusieurs dizaines de milliers de modems ont été mis hors service en France et en Europe. Cette coupure de communication satellitaire a privé plusieurs milliers de citoyens français de moyen de communication avec les services d'urgence et de secours. Des structures publiques ainsi que de nombreuses entreprises ont également été affectées. Le retour à un fonctionnement normal a pu prendre jusqu'à plusieurs mois pour certains clients français.

Elle a été attribuée à la Russie par l'Union européenne, dans une déclaration de son Haut Représentant pour les affaires étrangères et la politique de sécurité, le 10 mai 2022.

Source (août 2023) : Le satellite KA-SAT aurait dysfonctionné à cause d'une cyberattaque (usine-digitale.fr)

2.2.2 Une structuration récente de la lutte contre la cybercriminalité à conforter

Outre la protection des systèmes d'information contre les cyberattaques et l'action militaire, la Revue stratégique de cyberdéfense de 2018 identifiait deux autres chaînes opérationnelles essentielles à la cyberdéfense : le renseignement, pour faire face à l'espionnage d'État ou industriel, et l'investigation judiciaire, pour lutter contre la cybercriminalité. Les évolutions des cybermenaces montrent effectivement l'intérêt de coordonner ces quatre piliers de la sécurité nationale.

La progression de la menace cybercriminelle a amené une réorganisation des services judiciaires et des forces de l'ordre pour renforcer leur action. Si la refonte des services de police et de gendarmerie est encore trop récente pour être évaluée, la structuration du ministère de la justice reste à conforter et à mieux ancrer au sein de la gouvernance de la lutte contre les cybermenaces.

[56] Trois attributions publiques ont été réalisées par le Royaume-Uni en 2022 et une en 2023. Ce souci de transparence dépasse l'attribution des attaques. Ainsi, à la suite de la cyberattaque dont a été victime *la British Library* en octobre 2023, son directeur a publié en mars 2024 un rapport détaillé sur l'origine, la nature et les conséquences de l'attaque. Dans son rapport publié en janvier 2025 (*Government cyber resilience*), le National Audit Office indique que cette cyberattaque a généré un coût de 600 000 £ en mars 2024, la librairie indiquant que ce coût n'est pas définitif.

[57] Advanced Persistant Threat (APT) désigne un type d'attaque ou un groupe de personnes, souvent « sponsorisé » par un État. En l'occurrence, APT31 serait sponsorisé par la Chine.

2.2.2.1 Des réorganisations récentes des services de lutte contre la cybercriminalité au sein du ministère de l'intérieur

Dans la continuité du rapport Robert de 2014[58] qui soulignait déjà « *la nécessité d'une stratégie globale* (…) [et] *des réponses répressives plus effectives et davantage protectrices* », le ministère de l'intérieur a restructuré en 2023 les services de la police et de la gendarmerie nationales dédiés à la lutte contre la cybercriminalité, en cohérence avec les objectifs fixés dans le Livre blanc sur la sécurité intérieure de 2020 et de la loi de programmation et d'orientation du ministère de l'intérieur (LOPMI) 2023-2027[59]. Les objectifs sont ambitieux : plan d'investissement technologique, regroupement des capacités techniques et d'analyse, création d'une école de formation cyber interne, recrutement de 1500 cyberpatrouilleurs supplémentaires[60]. Dans le prolongement de ces plans ministériels, la police nationale s'est dotée, en 2022, d'un plan national cyber quinquennal de renforcement de la lutte contre la cybercriminalité qui prévoit une augmentation de 306 effectifs, la formation de 2450 spécialistes, et la création d'un service à compétence nationale, l'office anti-cybercriminalité (OFAC).

Au sein du ministère de l'intérieur, la lutte contre la cybercriminalité est partagée entre la police nationale, avec une action forte et déjà ancienne de la préfecture de police de Paris au travers de sa brigade de lutte contre la cybercriminalité (BL2C)[61], la gendarmerie nationale, et la direction générale de la sécurité intérieure (DGSI).

La direction générale de la sécurité intérieure, seule entité à pouvoir exercer sur le territoire national aussi bien dans un cadre judiciaire que de renseignement, est positionnée sur les menaces cyber en lien avec l'espionnage et l'ingérence, la prolifération, le terrorisme, les subversions violentes et la protection économique.

Les forces de police et de gendarmerie dédiées à la cybersécurité ont fait, quant à elles, l'objet d'une réorganisation, fin 2023. Le commandement de la gendarmerie dans le cyberespace (COMCyberGEND), créé en février 2021 pour animer et coordonner les capacités de la gendarmerie dans le domaine cyber, qu'il s'agisse de prévention, de formation ou d'investigations, a été transformé en commandement du ministère de l'intérieur dans le cyberespace (COMCYBER-MI)[62]. Service à compétence nationale, ses missions restent identiques mais sont étendues à l'ensemble du ministère[63]. Il est chargé, en particulier, d'assurer

---

[58] « Protéger les internautes », rapport sur la cybercriminalité, février 2014, procureur général Marc ROBERT, groupe de travail interministériel sur la lutte contre la cybercriminalité.
https://www.vie-publique.fr/rapport/34113-proteger-les-internautes-rapport-sur-la-cybercriminalite

[59] Loi n° 2023-22 du 24 janvier 2023.

[60] Les cyberpatrouilleurs peuvent réaliser certains actes d'enquête prévus par l'article 230-46 du code de procédure pénale. Ces enquêteurs sous pseudonyme (ESP) doivent être formés et habilités par l'autorité judiciaire. Initialement limitées aux atteintes aux mineurs commises via internet, leurs compétences ont été étendues à la détection des escroqueries et trafics en ligne, et leurs enquêtes élargies à toute infraction punie d'une peine d'emprisonnement commise par la voie des communications électroniques.

[61] La BL2C a succédé en 2019 à la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) créée en 1994. La BL2C disposait, début 2024, de 57 ETP.

[62] Décret n° 2023-1084 du 23 novembre 2023 portant création du service à compétence nationale dénommé commandement du ministère de l'intérieur dans le cyberespace.

[63] Le COMCYBER-MI a pour mission : d'élaborer la stratégie ministérielle de lutte contre la cybercriminalité ; d'animer, de coordonner et de suivre la mise en œuvre par les services du ministère de l'intérieur de la stratégie interministérielle de prévention des cybermenaces définie par les services du Premier ministre et de la stratégie

le soutien opérationnel et l'appui d'expertise[64] aux autres services du ministère dans le cadre d'enquêtes judiciaires, avec notamment une fonction de centralisation des informations et renseignement criminel pertinents pour l'intelligence cyber. Il dispose, en outre, du centre national de formation cyber (CNF-Cyber), créé le 1er août 2022 à Lille, qui propose des formations de haut niveau au profit des forces de sécurité intérieure, des autres ministères et des partenaires internationaux.

Malgré l'extension de son champ de mission, il est resté sous l'autorité du directeur général de la gendarmerie nationale et peine à attirer les compétences et le personnel des autres directions opérationnelles du ministère de l'intérieur[65], et la croissance de ses effectifs (de 134 civils et gendarmes initiaux à 166 ETP à l'été 2024) n'est réalisée, fin 2024, que par du personnel issu de la gendarmerie[66].

L'office anti-cybercriminalité (OFAC), créé également fin 2023[67], se substitue à la sous-direction de la lutte contre la cybercriminalité (SDLC) de la police nationale[68] et à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Pôle de compétence nationale, il est resté rattaché à la direction nationale de la police judiciaire (DNPJ). Il est chargé de lutter contre toutes les formes de cyberdélinquance, hors celles qui relèvent de la responsabilité de la DGSI. Service d'enquête, il est notamment responsable au niveau national de l'animation et de la coordination opérationnelle des services de lutte contre la cybercriminalité, en intégrant les missions d'enquête, d'appui, de renseignement et de détection. L'OFAC regroupait, au 30 avril 2024, 172 ETPT (dont 6 gendarmes), pour un effectif théorique de 196 ETPT.

Cette réorganisation sommitale des forces opérationnelles de lutte contre la cybercriminalité s'inscrit dans une continuité forte par rapport à l'organisation précédente. Il conviendra de s'assurer que l'objectif d'organiser la transversalité des compétences et des missions, notamment entre gendarmerie et police nationales est rempli. À cet égard, deux points de vigilance peuvent être relevés :

- l'unité nationale cyber (UNCyber), créée également fin 2023, est le service national d'enquête de la gendarmerie dédié à la cybercriminalité organisée. Elle a vocation à coordonner le dispositif cyber de la gendarmerie qui se met en place aux niveaux local (un spécialiste cyber par brigade), départemental (un à trois spécialistes cyber *forensic*) et régional, au sein des groupes interministériels de recherche (cinq à six spécialistes

ministérielle de lutte contre la cybercriminalité ; de produire chaque année un rapport d'état de la menace cyber du ministère de l'intérieur ; de coordonner les moyens capacitaires du ministère de l'intérieur et des outre-mer dans son domaine de compétence.

[64] Le COMCYBER-MI / SCN dispose d'une équipe d'enquêteurs experts projetables sur le territoire national.

[65] Le COMCYBER-MI a vocation à accueillir du personnel de la DGSI, de la préfecture de police de Paris et de la police nationale. Le DGGN a ainsi adressé un courrier en ce sens au DGPN et au DGSI, ainsi qu'au préfet de police de Paris en décembre 2023 (Lettres n°057245/GEND/CAB du 3 décembre 2023).

[66] La DGGN précise que « *la gendarmerie a effectivement comblé un maximum de postes de sous-officiers, notamment aux prix d'arbitrages au profit du COMCYBER*-MI » et qu'en ce qui concerne le personnel civil, « *elle a également comblé une vingtaine de postes grâce à des mobilités internes ou des arrivées extérieures de contractuels.* Le déficit en ressources humaines perdure donc, avec une contribution de la police nationale qui reste à arbitrer au niveau du ministère.

[67] Décret n° 2023-1083 du 23 novembre 2023 portant création de l'office anti-cybercriminalité.

[68] Arrêté du 29 avril 2014 modifiant l'arrêté du 5 août 2009 relatif aux missions et à l'organisation de la direction centrale de la police judiciaire.

cyber), pour un effectif affiché de 9000 à 9400 enquêteurs potentiels[69]. De son côté, l'OFAC s'appuiera à terme (2027) sur un maillage territorial composé de 56 antennes ou détachements auprès des services territoriaux (zonaux et départementaux) de la police nationale sur l'ensemble du territoire métropolitain et outre-mer[70]. Il conviendra de veiller à ce que la mise en place de ces deux structures d'animation et de soutien, positionnées dans chacune des chaînes de commandement, s'inscrivent effectivement dans la perspective de pilotages stratégique et opérationnel communs aux deux forces de l'ordre ;

- la question des laboratoires d'expertise devra également être considérée sous l'angle de la mise en commun des compétences. La police nationale dispose de 18 laboratoires de l'investigation opérationnelle numérique (LION) répartis sur l'ensemble du territoire national. Le COMCYBER-MI, quant à lui, continue d'abriter, au sein de sa division des enquêtes spécialisées, de la donnée et des investigations techniques (DEDT)[71], un centre national d'expertise numérique (CNENUM) qui recouvre trois laboratoires experts (laboratoire de la rétroconception, laboratoire du véhicule numérique, laboratoire d'extraction et d'analyse numérique).

2.2.2.2 La lutte contre la cybercriminalité au ministère de la justice : une montée en puissance effective à conforter

La lutte contre la cybercriminalité a conduit à créer des entités spécialisées au sein de l'administration centrale et du Parquet général dès 2014.

Une mission de prévention et de lutte contre la cybercriminalité a été créée en 2014 et positionnée au sein de la sous-direction de la justice pénale spécialisée (JPS) de la direction des affaires criminelles et des grâces (DACG). Elle est confiée à un magistrat, placé sous l'autorité directe du sous-directeur, et assisté d'un rédacteur contractuel ou d'un attaché d'administration. Dans le cadre de la déclinaison des missions de la DACG[72] dans le domaine cyber, elle anime principalement le réseau des référents cybercriminalité, déployé depuis 2020 au sein des huit juridictions interrégionales spécialisées (JIRS) et des juridictions locales (parquet, parquet général et cour d'appel).

La loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, a attribué au parquet du tribunal judiciaire de Paris « *une compétence nationale concurrente en matière d'atteintes aux STAD*[73] ». Cette section « cyber » est devenue la section J3 de la

[69] Le dispositif de la gendarmerie a été considérablement étoffé depuis deux ans avec la décentralisation des formations dans les régions de gendarmerie en 2023. Cela s'est traduit en quelques mois par une augmentation du nombre d'ESP habilités d'environ 400 à 1100. L'objectif de 1500 ESP que la gendarmerie s'est fixé dans son plan « Ambition Cyber » devrait être atteint en 2025.

[70] La police nationale disposait en 2021 de 226 investigateurs en cybercriminalité (ICC) déployés dans les directions zonales ou régionales de la police judiciaire (pour un objectif de 1509 ICC et de 45 détachements cyber départementaux en 2027).

[71] Cette division comprend également un département des enquêtes qui réalise des investigations sur les menées cybercriminelles du haut du spectre.

[72] La direction des affaires criminelles et des grâces élabore les normes en matière pénale. Elle établit et conduit les politiques publiques en matière pénale. Elle assure également la direction du Casier judiciaire national.

[73] Cf. article 706-72-1 du Code de procédure pénale.

juridiction nationale de lutte contre le crime organisé (JUNALCO) du parquet du tribunal judiciaire de Paris, lors de sa création en 2019.

En 2024, la section J3 du parquet de Paris était composée de cinq magistrats (soit deux de plus qu'en 2023), de trois greffières, d'une juriste assistante et de deux assistants spécialisés. À titre de comparaison, d'autres pays européens ont développé des unités spécialisées en matière de cybercriminalité comme, par exemple, le Portugal (7 procureurs spécialisés), l'Autriche (6 procureurs spécialisés), la Belgique (4 procureurs spécialisés au sein du parquet fédéral), ou encore la Norvège (5 procureurs spécialisés), les Pays Bas (7 procureurs spécialisés) et l'Allemagne (une centaine de procureurs spécialisés).

La section J3 du parquet du tribunal judiciaire de Paris (Source JUNALCO/J3, 2024)

La section J3 du parquet du tribunal judiciaire de Paris est compétente en matière de la lutte contre la cybercriminalité. Elle dispose de trois niveaux de compétence :

- la compétence territoriale classique sur le ressort de Paris ;
- la compétence concurrente nationale telle qu'elle résulte de l'art. 706-72-1 du code de procédure pénale en matière d'atteinte aux systèmes de traitement automatisé de données (articles 323-1 à 323-4-1) et de sabotage informatique (411-9 du code pénal) ;
- la compétence au titre de la JUNALCO (706-80 du CPP), s'agissant des affaires qui sont ou apparaîtraient d'une grande complexité (ex : SKY ECC).

Au titre de ses compétences, la section J3 dispose de plusieurs leviers d'action (leviers d'entrave) face à la menace cybercriminelle :

- l'émission de mandats de recherche et d'arrêts internationaux à l'encontre de cybercriminels ou d'individus ayant mis leurs ressources à la disposition de cybercriminels ;
- le démantèlement d'infrastructures de groupes cybercriminels ou de réseaux malveillants ;
- la saisie des avoirs criminels.

La saisie des avoirs criminels et en particulier des cryptomonnaies est systématiquement sollicitée par le parquet de Paris. Le droit français lui permet notamment grâce à la qualification de blanchiment de procéder à la saisie de l'entièreté du patrimoine du mis en cause. Une difficulté réside cependant dans l'obtention des mots de passe sécurisés du mis en cause lorsque ce dernier ne coopère pas.

Le 18 janvier 2023, l'opération de démantèlement d'une plateforme russophone d'échanges de crypto-actifs a permis la saisie de l'équivalent de 19 millions d'euros en crypto actifs. Début 2024, le montant des saisies en cours pour l'année 2023 s'élevait à 22 841 635,83 euros.

Depuis sa création en 2019, la section J3 traite un contentieux particulièrement technique, en évolution et augmentation continues. La judiciarisation de ce type de contentieux a connu une croissance exponentielle à partir de 2020, avec une explosion du nombre de dossiers transmis au titre de la compétence concurrente nationale (CCN).

Tableau n° 3 : Nombre d'enquêtes préliminaires ouvertes sur la période 2017-2022, au titre de la « compétence concurrente nationale » de la section J3

Type de dossier	2017	2018	2019	2020	2021	2022	2023
Total des saisines "CCN"	17	53	65	408	603	612	654
Evolution		*212%*	*23%*	*528%*	*48%*	*1%*	*7%*

Source : J3/JUNALCO

Enfin, il existe depuis 2023 une chambre spécialisée au siège du tribunal judiciaire de Paris[74].

Pour faire face aux évolutions de la cybercriminalité, aussi bien en volume qu'en nature, une dépêche du Garde des Sceaux en date du 9 juin 2021, véritable « doctrine d'emploi » pour les juridictions, a précisé le rôle des différents acteurs judiciaires en matière de traitement des affaires cybercriminelles selon trois cas de figure : 1/ traitement des atteintes aux systèmes de traitement automatisée des données (STAD) : 2/ traitements des atteintes aux STAD susceptibles d'être le fait de groupes terroristes ; 3/ traitement des infractions usant de vecteurs « cyber ». Il en résulte une articulation des compétences des juridictions locales, des JIRS et du tribunal judiciaire de Paris (J3/JUNALCO) en fonction de la nature et du degré de complexité de l'affaire. Cette organisation des compétences devra être évaluée pour s'assurer qu'elle répond aux enjeux d'une cybercriminalité très évolutive.

Enfin, la section J3 considère que des modifications de la procédure ou de la règlementation pénales permettraient de renforcer l'efficience de la lutte contre la cybercriminalité :

- la création d'une infraction de fraude informatique, définie comme : « *le fait pour toute personne de chercher à se procurer pour soi-même ou pour autrui, avec une intention frauduleuse, un avantage économique indu en tirant profit d'un dysfonctionnement d'un système de traitement automatisé de données*» ;
- le retrait de la référence au code de la consommation dans la définition de l'infraction visant les opérateurs de plateforme en ligne, à l'article 323-3-2 du code pénal[75], qui laissent réaliser des transactions illicites sur leur site, de sorte à conforter les poursuites les concernant ;
- l'adaptation du code de procédure pénale afin de faire correspondre le cadre juridique aux nouvelles pratiques d'enquête [76] pour identifier les cybercriminels et qui posent, aujourd'hui, de très nombreuses questions procédurales, car les textes existants n'épousent pas avec exactitude les moyens utilisés par les policiers et les gendarmes.

Il apparaît nécessaire d'avancer rapidement sur les mesures à prendre en termes d'organisation des services judiciaires, de formation des services enquêteurs, d'adaptation du cadre législatif et des procédures pour certains actes d'investigation, comme des moyens à y consacrer par les ministères en charge de la lutte contre la cybercriminalité.

[74] S'agissant des magistrats du siège, les dossiers de la section J3 sont confiés aux juges d'instruction composant le pôle économique et financier du Tribunal judiciaire de Paris. Les dossiers sont jugés devant la 13e chambre correctionnelle.

[75] La LOPMI 2023-2027 a créé à l'article 323-3-2 du code pénal une nouvelle infraction sanctionnant le fait pour un opérateur de plateforme, utilisant notamment un moyen d'anonymisation des connexions (ex : TOR), de permettre des transactions illicites.

[76] Utilisation des nouvelles technologies, comme les techniques de copie-live, de redirection de flux, de désanonymisation de *Guard Nod* et même de copie de serveurs chez un hébergeur.

2.2.2.3 Un renforcement de la coopération avec les services de renseignement

La lutte contre la cybercriminalité demande un renforcement des échanges d'informations entre les services de renseignement et la section J3/JUNALCO. L'introduction en 2021 d'un nouvel article (706-105-1) dans le code de procédure pénale[77] répond en partie à cette problématique en organisant le transfert d'informations de la sphère judiciaire vers les services de renseignement. Cependant, cette passerelle doit fonctionner dans les deux sens pour actionner, en concertation, le bon levier pour traiter la cyberattaque (vecteur judiciaire ou autre) et mieux intégrer dans les procès-verbaux la contextualisation de l'attaque.

De tels échanges d'informations se développent désormais entre le ministère de l'intérieur et le ministère de la justice, au travers notamment de l'émission d'alertes sur les cybermenaces émises par le COMCYBER-MI ou le service d'information, de renseignement et d'analyse stratégique de la criminalité organisée (SIRASCO)[78].

La création d'une base de données dédiée aux infractions pénales en matière d'intrusion informatique[79], mise en œuvre depuis le 22 décembre 2021, vise à fluidifier les échanges avec la police et la gendarmerie nationales et à constituer un outil de partage d'informations sur les logiciels malveillants et indicateurs de compromission, à des fins de prévention, de recherche, de constatation ou de poursuite. Cependant, il conviendrait, d'une part, d'ouvrir ce traitement des données à un plus grand nombre de services investis dans la lutte contre la cybercriminalité, sous réserve de faisabilité technique, et, d'autre part, de structurer les données et d'organiser des modalités d'alimentation du dispositif plus rigoureuses de sorte à renforcer son efficacité.

Le traitement de la menace cybercriminelle n'appelle pas une réponse exclusivement judiciaire ou administrative. Il s'applique à des organisations transverses et impose une bonne articulation entre les interventions des différents services de l'État concernés. C'est pour élaborer ces réponses transverses qu'un comité judiciaire opérationnel (CJudOps), équivalent du C4 TechOps mais pour les sujets de cybercriminalité, a été mis en place officiellement en 2022, après sa préfiguration dès 2020. Placé sous la responsabilité de la sous-direction de la lutte contre la cybercriminalité (ministère de l'intérieur), intégrée depuis dans l'office anti-cybercriminalité (OFAC), il a vocation à se réunir mensuellement. Pour autant, en pratique, le fonctionnement de cette instance ne satisfait pas les besoins opérationnels des participants, qui nécessitent d'échanger des informations sur des affaires particulières, dans un cadre qui doit demeurer confidentiel. À ce titre, le format et le rattachement du CJudOps méritent d'être étudiés.

---

[77] Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, qui introduit dans le code de procédure pénale (CPP) un nouvel article 706-105-1, dérogatoire à l'article 11 du CPP, dans le cadre de la lutte contre la cybercriminalité et le haut du spectre de la criminalité organisée. La dépêche du 10 août 2021 du ministère de la justice précise les conditions d'application de ce nouvel article du CPP.

[78] Le SIRASCO est le service de renseignement criminel de la direction nationale de la police judiciaire. Il est constitué d'un service central composé de secteurs d'analyse géographique dédiés aux groupes criminels transnationaux, d'unités dans les offices centraux spécialisées sur une thématique criminelle (trafic de stupéfiants, criminalité financière, grand banditisme, cybercriminalité…) et d'antennes et détachements dans les territoires. Les analystes du SIRASCO ont pour mission de collecter, capitaliser et analyser les données réceptionnées ou recueillies dans le cadre du renseignement. Ils sont en lien étroit avec les services d'enquêtes et des services partenaires au niveau national et international.

[79] À partir du logiciel dénommé « Malware Information Sharing Platform - MISP-PJ ».

Recommandation n°2. (SGDSN, ministère de la justice, ministère de l'intérieur) En matière de lutte contre la cybercriminalité, renforcer la coordination entre les autorités judiciaires et les services de renseignement.

2.3 Des instances de pilotage de la sécurité numérique de l'État et de la cybersécurité de la société, récemment organisées, à renforcer

Les deuxième et troisième piliers de la politique de cybersécurité, visant respectivement à sécuriser l'État et à protéger les citoyens, sont soumis à une gouvernance spécifique, et restent insuffisamment pilotés par le SGDSN.

2.3.1 La politique de sécurité des systèmes d'information de l'État, une structuration récente sans traduction budgétaire

La stratégie de sécurité numérique de l'État n'a été structurée, sous la forme de l'instruction générale interministérielle (IGI) n°1337, qu'à l'été 2021[80], à la demande expresse du Premier ministre, à l'issue d'une inspection générale interministérielle qui en avait montré les limites.

Elle est distincte de la stratégie numérique de l'État : celle-ci relève, en effet, de la direction interministérielle du numérique (DINUM), service du Premier ministre, placé sous l'autorité du ministre de la transformation et de la fonction publiques[81] quand la cybersécurité de l'État est gouvernée, sous l'autorité du Premier ministre, par le SGDSN et son service à compétence nationale, l'ANSSI. Les interactions entre l'ANSSI et la DINUM sont établies dans chacun des textes d'organisation : l'ANSSI « *accompagne* »[82] la DINUM dans ses missions et la DINUM « *s'assure de la bonne prise en compte de la politique de sécurité numérique de l'État dans cette stratégie* [numérique de l'État] *ainsi que dans les différents projets qui lui sont soumis au titre de cette stratégie et de ses attributions* » et les responsables de la DINUM et de l'ANSSI participent aux instances de préparation des décisions[83] mais le pilotage reste différent.

En vertu de l'IGI 1337, les décisions stratégiques sont prises en réunions interministérielles (RIM) relatives à la cybersécurité, organisées à l'initiative du Premier ministre au minimum une fois par an.

Pour préparer ces décisions stratégiques, un comité stratégique interministériel de la sécurité numérique (COSINUS)[84], présidé par le secrétaire général de la défense et de la sécurité

[80] Publiée en annexe de l'arrêté du 26 octobre 2022 mais mise en œuvre dès l'été 2021.
[81] Référence DINUM, courrier à la Cour du 7 janvier 2025.
[82] L'ANSSI participe notamment aux instances de gouvernance de la stratégie numérique de l'État (comité stratégique interministériel du numérique – COSINUM - et comité interministériel de pilotage du numérique - CINUM).
[83] La DINUM participe au COSINUS et le DG ANSSI au COSINUM, instance de préparation de la stratégie numérique.
[84] L'ANSSI en assure le secrétariat.

nationale et composé des hauts fonctionnaires de défense et de sécurité (HFDS) de chaque ministère, de la directrice interministérielle du numérique et du directeur général de l'ANSSI, se réunit au minimum une fois par an. Le SGDSN et chaque HFDS présentent le niveau de sécurité numérique pour leur domaine de responsabilité et les plans d'actions associés ainsi qu'une synthèse sur les incidents de sécurité subis. Le directeur général de l'ANSSI présente un état de la cybermenace. Le COSINUS peut proposer, à l'issue, la révision du plan d'action des ministères, voire la modification de la politique de sécurité des systèmes d'information de l'État (PSSIE). Il définit la feuille de route interministérielle à valider en RIM.

L'IGI 1337 prévoit également la tenue de comités interministériels de pilotage de la sécurité numérique (CINUS), présidés par le directeur général de l'ANSSI et composés des fonctionnaires de la sécurité des systèmes d'information (FSSI) de chaque ministère. Sont également conviés des représentants des services de la présidence de la République, de l'Assemblée nationale, du Sénat et de la DINUM qualifiés sur les sujets relatifs au pilotage de la sécurité numérique. Les CINUS suivent la mise en œuvre de la feuille de route applicable aux ministères et sont des instances de partage et de réflexion sur les difficultés éventuellement rencontrées. Ils sont réunis sur une base mensuelle et en tant que de besoin.

Pour autant, la traduction concrète et le suivi des réalisations apparaissent perfectibles.

Un plan d'action a été décidé en réunion interministérielle du 30 août 2021 et il fait l'objet d'un suivi resserré à partir d'un tableau de bord établi par l'ANSSI, en concertation avec les ministères. Une dizaine d'indicateurs sont suivis en 2023. Ils sont assortis d'une évaluation selon un code couleur quaternaire (vert, jaune, orange et rouge), voire d'une note.

Ce suivi régulier, assorti des mesures d'aides financées par le plan de relance post-Covid, notamment dans le cadre du programme TEMPO, a permis une amélioration de la sécurisation des systèmes d'information. Toutefois, les indicateurs concernent des points de sécurité relativement basiques, ou des actions qui, une fois mises en place, n'appellent pas d'évolutions. C'est le cas, par exemple, de la mise en place d'« une capacité d'alerte et de réaction aux cyberattaques » qui passe du vert à la mise en place d'un CSIRT ministériel. Ces indicateurs doivent donc évoluer pour refléter une dynamique de sécurisation.

Le tableau de bord permet, par ailleurs, de constater que tous les ministères conservent des marges de progression significatives fin 2023 sur des sujets structurants, notamment dans l'homologation des systèmes d'information soutenant des missions essentielles, le remplacement des éléments obsolètes et le traitement du volet cybersécurité dans les plans de continuité ou de reprise de l'activité. La gouvernance rapprochée n'a, pour autant, pas débouché sur l'établissement d'un schéma directeur, concerté avec les ministères, pluriannuel et précisant les crédits et effectifs nécessaires.

La « feuille de route des efforts prioritaires en matière de sécurité numérique pour 2023-2024 » établie par l'ANSSI à l'échelle interministérielle ne contient que la mise en œuvre de mesures basiques de sécurité, sans distinguer entre les différentes entités ni déterminer d'échéancier de ressources humaines ou financières.

Du reste, alors que le positionnement de cette comitologie était défini expressément « *en amont des dialogues de gestion budgétaire* » par l'IGI 1337, laissant entendre que les décisions devaient être prises en compte dans les crédits accordés aux entités publiques, les COSINUS des 16 mars 2022 et 6 juin 2023 ne mentionnent pas les sujets budgétaires, seulement l'affectation de crédits supplémentaires issus du plan de relance (cf. *infra*).

2.3.2 Une gouvernance partagée de la politique économique en faveur de la cybersécurité

Dans ce volet de la lutte contre les cybermenaces en direction de l'ensemble de la société, le pilotage des actions de l'État est multiple.

Outre les actions couramment portées par les différents ministères en matière de recherche, de formation, ou de soutien à l'économie, l'État a défini une politique industrielle en faveur de la sécurité numérique, au travers de la « Stratégie nationale d'accélération pour la cybersécurité » lancée en février 2021, dans le cadre du plan d'investissement d'avenir (PIA) 4, puis intégrée dans le plan d'investissement France 2030.

Cette stratégie est pilotée par le secrétariat général pour l'investissement (SGPI), service du Premier ministre, au travers des opérateurs conventionnés[85] et la cybersécurité est suivie par un coordonnateur dédié.

Les relations entre ce coordonnateur et l'ANSSI sont fortes et régulières. L'ANSSI est ainsi associée aux processus de sélection des projets financés au titre de cette stratégie, notamment ceux portés par des entreprises privées. En effet, les objectifs de la stratégie sont focalisés sur le déploiement de la filière économique, à l'horizon 2025 : triplement du chiffre d'affaires de 2019, doublement des emplois dans le secteur et émergence de trois licornes françaises en cybersécurité.

Ce financement de l'offre de produits et services sensibles relève de la problématique de la souveraineté nationale.

En effet, selon les données communiquées par le SGPI, à partir du baromètre Tikehau, société gestionnaire d'actifs, qui a notamment repris le fonds d'investissement Brienne dédié au secteur de la cybersécurité, 38 jeunes entreprises en phase de création (start-up) ou de croissance (scale-up[86]) dans ce domaine ont réussi des levées de fonds pour un total de 338 M€. Ces opérations réalisent un des objectifs du plan France 2030 et concrétisent l'effet levier des aides publiques recherché.

Cependant, ces levées de fonds peuvent entraîner la prise de contrôle de solutions de cybersécurité sensibles par des acteurs étrangers. À ce titre, elles entrent dans le dispositif de contrôle des investissements étrangers en France (IEF), piloté par la direction générale du Trésor (DGT), sur le fondement des articles L151-3 et R151-3 du code monétaire et financier, visant à préserver la souveraineté nationale.

Le bouclage avec la gouvernance de la cybersécurité civile s'opère au travers des sollicitations, par la DGT, des avis de l'ANSSI sur les demandes d'autorisation d'investissements étrangers.

---

[85] En vertu de la convention du 2 juin 2021 entre l'État, l'agence nationale de la recherche (ANR), l'ADEME, l'EPIC Bpifrance et la société anonyme Bpifrance, relative au programme d'investissements d'avenir.

[86] Une start-up est une jeune entreprise en phase de création qui cherche à faire valider son produit sur le marché et obtenir des financements. Une scale-up a son produit validé sur le marché, emploie au moins 10 personnes, affiche un taux de croissance d'au moins 20 % sur les trois dernières années et un chiffre d'affaires entre 1 et 3 millions d'euros.

Tableau n° 4 : Nombre de dossiers transmis par la DGT pour avis de l'ANSSI

	2018	2019	2020	2021	2022	2023
Sollicitations de l'ANSSI	25	32	55	70	51	52

Source : ANSSI

Le nombre de sollicitations effectuées au cours des exercices récents n'a cessé de croître entre 2019 et 2021 (+ 34 % en 2019, + 72 % en 2020, + 27 % en 2021), en lien avec l'accroissement des opérations de fusion-acquisition dues aux opportunités économiques engendrées par la crise sanitaire et par l'extension du champ d'application de la réglementation IEF. En 2022, la diminution de près de 27 % du nombre de dossiers soumis est liée, notamment, au reflux des opportunités économiques mais également, selon l'ANSSI, à une meilleure connaissance de son périmètre d'expertise, par le bureau en charge de ces dossiers à la DGT. En 2023, le nombre de sollicitations transmises à l'ANSSI est stable. Pour autant, l'ANSSI considère qu'un nombre important de sollicitations ne relève pas réellement de son champ d'expertise, du fait du renouvellement important des effectifs au sein du bureau concerné de la DGT. Ces constats démontrent que les relations entre les deux sphères de l'État, économique et de sécurité, en matière de pilotage de la cybersécurité peuvent être améliorées.

Cette régulation est nécessaire compte tenu de la sensibilité de certaines solutions de cybersécurité, d'autant plus qu'elles bénéficient parfois d'aides au titre du plan France 2030, de la labellisation de leur solution par l'ANSSI (ce qui leur confère une forte légitimité et l'accès aux OIV), et, dans un certain nombre de cas, de leur inscription au catalogue de l'Union des groupements d'achats publics (UGAP)[87]. Ce soutien public multiforme à des start-ups doit avoir pour contrepartie, si l'intérêt stratégique des solutions est établi, un ancrage national des sociétés productrices.

L'existence de multiples politiques publiques touchant la cybersécurité et la sensibilité particulière de certaines solutions techniques soulignent l'intérêt de renforcer la coordination opérée, au niveau du Premier ministre, par le SGDSN, dans ce pilier de la lutte contre les cybermenaces. La nouvelle stratégie nationale de cybersécurité de 2024 préconise, judicieusement, de confier le pilotage interministériel des politiques publiques afférentes au SGDSN, adossé à un comité de pilotage des politiques publiques cyber (C3PC).

CONCLUSION INTERMÉDIAIRE

La lutte contre les cybermenaces a été intégrée dans le dispositif de gouvernance en matière de défense, au plus haut niveau de l'État. La structuration de la politique de cybersécurité en trois volets d'actions - réponse aux cyberattaques, renforcement de la sécurité des systèmes d'information de l'État, et protection numérique de la société -, conformément

[87] Le 7 mai 2015, une convention entre l'ANSSI, et l'UGAP a été signée visant à faire mieux connaître les produits et prestations labellisés par l'ANSSI et en faciliter l'achat par les collectivités publiques. Dans ce cadre, l'ANSSI est associée à la rédaction des cahiers des charges des procédures mises en place par la centrale d'achat public portant sur l'acquisition de produits de sécurité des systèmes d'information ainsi que de services de confiance. En retour, l'UGAP veille à la visibilité des produits labellisés par l'ANSSI dans les supports de communication de ses offres d'équipements sécurité réseaux et de logiciels (catalogues, ugap.fr...).

aux orientations définies par la Revue stratégique de cyberdéfense de 2018, a renforcé le pilotage interministériel des chaînes de décision, sans pour autant l'unifier. Si les caractéristiques particulières de chacun des volets justifient des organisations spécifiques de leurs gouvernances, il apparaît toutefois nécessaire de définir une capacité de supervision, pour assurer la complémentarité des actions publiques mais également veiller à la sécurité de leur réalisation dans un domaine sensible. La Revue stratégique de cybersécurité de 2024 préconise le maintien d'un « comité directeur cyber », présidé par le Premier ministre, avec l'assistance du SGDSN, traitant des trois volets de la sécurité numérique pour définir les grandes orientations de l'État en matière de cybersécurité et suivre la mise en œuvre des décisions prises en conseil de défense et de sécurité nationale. Sa mise en place devra être rapidement effective.

Dans le domaine de la réponse aux cyberattaques, la montée en capacité du ministère des affaires étrangères pour porter la voix de la France dans les instances internationales de régulation du cyberespace permettra d'affiner la décision d'identifier les État agresseurs en prenant mieux en comptes les exigences diplomatiques. La structuration récente des services de lutte contre la cybercriminalité doit, par ailleurs, aboutir à une meilleure articulation opérationnelle entre les enquêtes conduites par les services de renseignement et dans le cadre judiciaire pour faire jouer à plein le levier des sanctions pénales.

Dans le domaine de la sécurité numérique des services de l'État, une attention particulière devra être portée à la traduction budgétaire de la programmation des opérations nécessaires au renforcement de la cybersécurité.

Dans le domaine de la politique économique, l'accompagnement de l'émergence de solutions et produits de cybersécurité doit mieux prendre en compte les besoins des utilisateurs, d'une part, s'inscrire plus solidement dans le cadre réglementaire défini pour conforter la souveraineté nationale, d'autre part.

---

3 UN DEVELOPPEMENT DE L'ANSSI A MIEUX ENCADRER

L'ANSSI a été créée par décret n° 2009-834 du 7 juillet 2009, modifié à différentes reprises. Les missions qui lui ont été assignées couvrent l'ensemble du champ de la cybersécurité civile. Face aux mutations et à l'ampleur de la menace, sa croissance continue et les réorganisations internes ne suffiront plus. Il est désormais nécessaire d'adapter les missions et les modalités d'action de cet opérateur central, aux exigences résultant de l'évolution des menaces. En effet, alors qu'elle s'adressait à un nombre d'acteurs réduit, l'ANSSI est désormais une autorité de régulation pour un large spectre d'entités dont le niveau de maturité en matière de cybersécurité est pour le moins hétérogène.

3.1 Des fonctions à conforter par la mobilisation et la coordination d'autres prestataires

Face aux mutations des cybermenaces, aux évolutions de la réglementation européenne et à la nouvelle stratégie de cybersécurité, l'organisation de certaines missions de l'ANSSI doit être revue.

3.1.1 L'assistance technique de l'ANSSI, une organisation à calibrer au plus proche des besoins des bénéficiaires

La division « assistance technique » (DAT) de la sous-direction de l'expertise (SDE) de l'ANSSI assure, parmi ses missions, un soutien technique aux administrations et aux opérateurs d'importance vitale, aux opérateurs de services essentiels et aux fournisseurs de services numériques, pour la conception et la mise en œuvre de leurs systèmes d'information les plus critiques. Cette activité est réalisée par 34 ETPT.

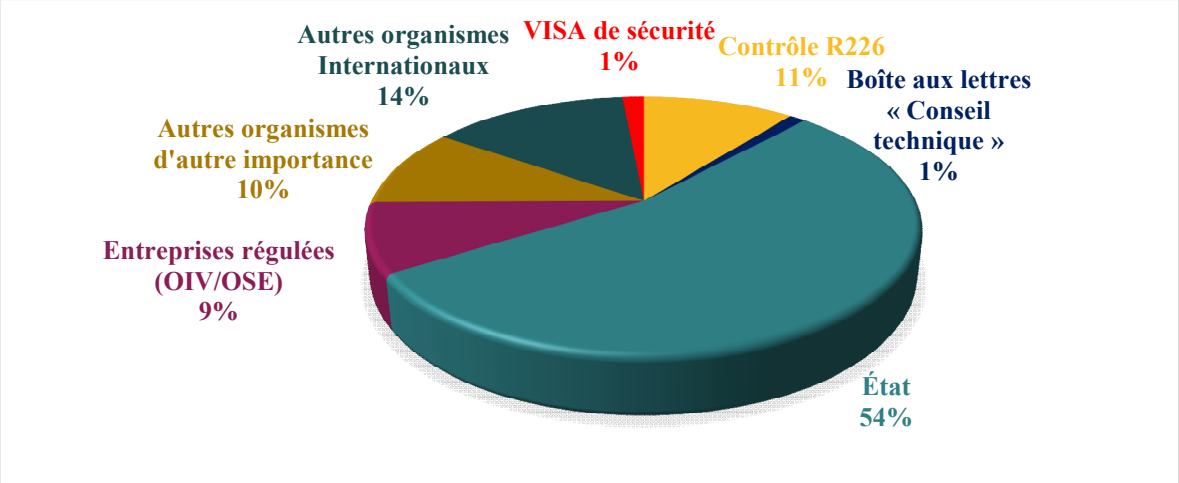
La gestion des sollicitations techniques de premier niveau est réalisée au travers de la messagerie « conseil technique ». Cette activité est réalisée en puisant sur les disponibilités des agents : quatre collaborateurs de la DAT contribuent à répondre aux sollicitations, selon un « contrat d'engagement » qui consiste à consacrer au maximum huit heures par semaine pour le traitement de ces demandes. En 2023, l'activité « conseil technique » a mobilisé 333 heures de travail pour 131 demandes. Le délai moyen de réponse est de cinq jours, et le délai maximum de 15 jours.

Aucune étude n'a cependant été réalisée sur l'adéquation de ce dispositif aux besoins des utilisateurs et il n'existe pas d'indicateur de satisfaction « client ». Il serait également nécessaire de s'assurer de la pertinence de l'organisation du dispositif, le niveau élevé d'expertise des agents de la SDE invitant à consacrer cette ressource rare et coûteuse à des prestations complexes.

Au-delà de ces sollicitations de premier niveau, l'ANSSI produit une assistance technique plus appuyée à différentes entités. L'assistance consacrée aux services de l'État est majoritaire et celle consacrée aux OIV / OSE plus marginale. Une part significative de

l'assistance technique est offerte à des organismes internationaux. Les 29 037 heures consacrées à la mission d'assistance technique en 2023 se déclinent de la manière suivante :

Graphique n° 1 : Répartition des heures d'assistance technique par type de bénéficiaires en 2023



*Source : ANSSI - *R 226-1 du code pénal et suivants sur la détention d'appareils d'interception et d'analyse de données*

Les principaux bénéficiaires sont donc des services de l'État. L'assistance qui leur a été portée représente 25 % des heures réalisées dans l'année.

Tableau n° 5 : Principaux bénéficiaires de l'assistance technique de l'ANSSI en 2023

Ministères	Nombre d'heures de travail
Services du Premier ministre	3 176
Ministère de l'intérieur	2 054
Ministère des armées	786
Ministère de l'Europe et des affaires étrangères	657
Ministères sociaux	612
Total général	**7 285**

Source : ANSSI

Le processus d'assistance technique s'inscrit dans une logique de flux des demandes. Pour chaque assistance technique, un objectif opérationnel est défini avec le bénéficiaire. Le délai d'instruction et la nature du soutien dépendent de plusieurs facteurs, parmi lesquels le contexte et les besoins du bénéficiaire (projet, assistance post incident, etc.), le type et la complexité du système d'information étudié, les délais et moyens engagés par le bénéficiaire lui-même, les ressources et priorités internes à l'agence, etc. Le spectre de l'assistance va de l'engagement simple - une ou deux réunions de trois heures avec le bénéficiaire pour partager

sur des orientations techniques (compte rendu à l'appui) – à l'intégration d'experts de la DAT dans les équipes techniques du bénéficiaire afin d'aider de manière opérationnelle[88].

Il n'existe pas de dispositif d'enregistrement des demandes adressées à l'ANSSI. Il est donc difficile de mesurer leur taux de prise en charge. L'étiage des réalisations est passé de près de 230 à moins de 150 entre 2019-2020 et 2021-2022. Le nombre d'assistances réalisées en 2023 est remonté à 173, tout type d'assistance confondu (hors conseil ponctuel). Le sous-directeur de l'expertise considère que le potentiel réel de l'ANSSI est proche de 80 assistances techniques de moyenne ampleur par an. La mise en place d'un processus de programmation annuel ou pluriannuel, ajusté aux besoins et établi en concertation avec les bénéficiaires potentiels, permettrait de prioriser la validation des demandes, quitte à procéder à une réorientation de celles d'entre elles qui n'exigent pas un niveau d'expertise très élevé vers d'autres prestataires.

3.1.2 Une qualification de produits et de services par l'ANSSI à faire évoluer

L'ANSSI renforce la confiance des utilisateurs en mettant en place des procédures de qualification et de certification[89] visant à évaluer et à approuver les produits, services et prestataires de cybersécurité qui répondent à ses normes et exigences.

Deux types de certifications sont proposés, la certification « critères communs » (CC) selon un standard internationalement reconnu qui s'appuie sur des accords de reconnaissance multilatéraux ; la certification de sécurité de premier niveau (CSPN), introduite par l'ANSSI pour offrir une alternative aux évaluations « critères communs », en évaluant la résistance d'un produit face à des attaques de niveau modéré[90]. Le processus d'évaluation est réalisé par des centres d'évaluation de la sécurité des technologies de l'information (CESTI), laboratoires privés, qui doivent être accrédités selon la norme ISO/IEC 17025 par le comité français d'accréditation (Cofrac)[91] et agréés par l'ANSSI pour les évaluations CC et CSPN. Une certification n'est valable que pour une version donnée d'un produit.

La qualification ANSSI est divisée en trois niveaux pour les produits de sécurité (élémentaire, standard et renforcée), chacun représentant un degré de résistance aux

[88] Ce niveau de soutien n'est ouvert qu'aux services de l'État.

[89] La certification est une attestation du degré de robustesse d'un produit, établie grâce à une analyse de conformité et à des tests de pénétration effectués par un évaluateur tiers sous la supervision de l'ANSSI, selon des schémas et référentiels adaptés aux besoins de sécurité des utilisateurs et prenant en compte les avancées technologiques. La qualification est un processus de recommandation par l'État français de produits ou services de cybersécurité qui ont été testés et approuvés par l'ANSSI. Cette approbation atteste que ces produits ou services sont conformes aux exigences règlementaires, techniques et de sécurité, établies par l'ANSSI, ce qui garantit leur robustesse et la compétence du prestataire de service. Elle valide également la capacité du fournisseur à respecter sur le long terme un ensemble d'engagements pris envers l'ANSSI. Pour les produits, cela peut inclure la confidentialité et la protection des données, ainsi que la correction des failles et des vulnérabilités. Pour les services, cela peut inclure le maintien des compétences du prestataire par exemple La qualification d'un produit ou d'un service par l'ANSSI est reconnue en France et, selon certains cadres règlementaires, en Europe.

[90] La CSPN est généralement moins exhaustive que la certification CC et se concentre davantage sur l'analyse du produit. Elle consiste en des tests réalisés dans des conditions de temps et de charge contraintes (généralement 2 mois, 25 à 35 jours/homme).

[91] Le Cofrac est une association à but non lucratif, chargée par les pouvoirs publics de délivrer les accréditations aux organismes intervenant dans l'évaluation de la conformité en France.

cyberattaques. La qualification des services est réalisée selon la catégorie d'utilisation : audit, réponse aux incidents, détection des incidents, informatique en nuage et services de confiance numérique. Selon le cadre règlementaire, la qualification est octroyée pour une durée maximale de deux à trois ans.

Le processus est obligatoire pour les solutions destinées à équiper les OIV, les autorités administratives relevant du référentiel général de sécurité (RGS)[92] et les entités relevant du règlement « *electronic Identification, Authentication and Trust Services* » (eIDAS - « Services électroniques d'identification, d'authentification et de confiance »). Il est un atout commercial pour les autres entités qui peuvent ainsi afficher un niveau élevé de sécurité de leurs solutions. Il a un coût pour les fabricants de solutions de cybersécurité qui se répercute sur leur prix.

Tableau n° 6 : Coûts indicatifs des procédures d'évaluation

Type	Durée	Coût de l'évaluation (hors coûts internes)
CSPN	de 6 à 10 mois	Entre 35 et 50 K€
CC	de 12 à 18 mois	Entre 50 et 300 K€
Qualification de produit	de 12 à 24 mois	Entre 35 et 300 K€
Qualification de service	de 8 à 18 mois	Entre 50 et 150 K€

Source : ANSSI

La mise en œuvre des différents dispositifs de qualification[93] représente un engagement significatif pour l'ANSSI, qui y consacre une trentaine d'ETP.

Tableau n° 7 : Activités de qualification de l'ANSSI

	2019	2020	2021	2022	2023
Visas de sécurité	263	254	257	331	317
dont qualifications	168	140	169	240	230
dont qualification de produits	28	36	30	37	62
dont qualification de prestataires	140	104	139	203	168
dont certifications	95	114	88	91	87
Nombre de qualifications de produits depuis 2015					273
Nombre de qualifications de prestataires depuis 2015					585
Nombre de certifications depuis 2015					475
Nombre de centres d'évaluation agréés en 2015					10

Source : ANSSI

[92] Prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives. Ses conditions d'élaboration, d'approbation, de modification et de publication sont fixées par le décret no 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance citée relatifs à la sécurité des informations échangées par voie électronique.

[93] Par ailleurs, l'ANSSI délivre deux labels, attestant de la conformité à un cahier des charges, validée directement par l'ANSSI elle-même : le label *Ebios Risk Manager* et le label *SecNumEdu* pour les formations. La liste des produits et services qualifiés sont sur le site internet de l'ANSSI.

Outre son coût élevé, le processus de qualification connaît différentes limites : il répond à une logique de guichet - la demande de visas étant à l'initiative des offreurs de solution - et rend complexe une approche par besoins des utilisateurs ; il est par ailleurs exigeant en temps et pose donc un problème de rythme de qualification.

Des pistes sont à l'étude au sein de la sous-direction de l'expertise de l'ANSSI pour fluidifier le dispositif. Concernant la qualification de service, il est prévu de distinguer à l'avenir deux niveaux : élevé et substantiel. Cette évolution sera mise en œuvre dans un premier temps pour les qualifications « prestataires d'audit de sécurité (PASSI) » et « prestataires de réponse aux incidents de sécurité (PRIS) », permettant ainsi de mieux répondre aux différents besoins des utilisateurs. Cette évolution permet aussi d'anticiper la transition vers la certification européenne suite à l'accord trouvé au niveau de l'Union européenne sur l'amendement du *Cybersecurity Act* pour lequel la Commission a jugé que l'approche française utilisant le levier de la qualification de prestataires de service était le plus pertinent pour servir de modèle au niveau européen. De plus, l'ANSSI peut déléguer, sous certaines conditions, la qualification de services au niveau substantiel à des organismes tiers accrédités, ce qui permet de fluidifier le processus.

Concernant la qualification de produits, des évolutions ont été réalisées pour qu'elle soit applicable aux versions ultérieures d'un produit permettant ainsi de s'assurer d'un bon rythme de qualification notamment dans le cas de l'apparition d'un patch. La démarche bénéficiera également des évolutions du process de certification de produits qui font consensus au niveau européen.

Par ailleurs, l'ANSSI réfléchit au dispositif le plus adapté pour répondre aux besoins de recommandation de ses bénéficiaires sur une gamme de produits plus étendue et dans des délais plus courts. Il convient de faire aboutir rapidement ces travaux pour accroître la transparence du marché des produits de cybersécurité.

3.1.3 La remédiation aux cyberattaques, un dispositif élargi récemment

3.1.3.1 Un CERT-FR confronté à des cyberattaques plus nombreuses et chronophages

L'ANSSI est le centre de réponse aux incidents de sécurité gouvernemental et national français (CERT-FR[94]). Le CERT-FR est porté par la sous-direction des opérations de l'ANSSI.

[94] *Computer Emergency Response Team*. Les missions du CERT-FR sont les suivantes : répondre aux demandes d'assistance suite aux incidents de sécurité sur les réseaux et les systèmes d'information de ses bénéficiaires. Il traite ainsi la réception des demandes, l'analyse des symptômes des incidents, l'identification d'éventuelles corrélations avec d'autres incidents similaires et la définition de solutions de reprise après incident ; traiter les alertes et réagir aux attaques informatiques ; détecter les attaques ciblant les systèmes d'information gouvernementaux, grâce à un service permanent de supervision de la sécurité au profit des services de l'État ; détecter les vulnérabilités des systèmes, au travers notamment d'une veille technologique sur les produits majeurs du marché ; contribuer à la prévention des attaques informatiques, en diffusant des informations sur les précautions à prendre pour réduire les risques d'incidents et minimiser leurs conséquences éventuelles ; coordonner la prévention et la réponse à incidents avec les entités partenaires.

Tableau n° 8 : Données d'activité de défense de l'ANSSI

	2019	2020	2021	2022	2023
Signalements	2 296	2 287	3098	3029	3315
Signalement traités	1917	1520	2019	2173	2195
En % de signalements	83,5 %	66,5 %	65,2 %	71,7 %	66,2 %
Incidents	370	759	1057	831	1100
dont majeurs	9	7	5	3	3
Opérations de cyberdéfense	16	20	17	21	17

Source : ANSSI

Si le nombre d'incidents majeurs ou d'opérations de cyberdéfense peut sembler restreint, l'ANSSI souligne toutefois le caractère chronophage de deux types d'actions de remédiation : le repérage des outils furtifs de l'espionnage étatique et les opérations réalisées en urgence auprès d'acteurs sensibles, notamment dans le secteur de la santé, qui appellent l'apport rapide d'une aide aux victimes mais également un suivi continu, notamment en heures non ouvrées. Elle considère que la complexité des opérations d'endiguement, de remédiation ou de gestion d'une crise est croissante, du fait de l'élargissement des menaces à l'ensemble de la chaîne d'approvisionnement de ses bénéficiaires.

Cette tendance se double d'une attente accrue des bénéficiaires de l'agence, qui souhaitent non seulement une intervention technique de remédiation rapide, mais également une prestation d'accompagnement en vue du maintien de leurs activités. Dans cette perspective, une bonne connaissance des métiers des victimes, et donc des contraintes liées à leur secteur, tend ainsi à être un élément majeur des opérations de sécurisation et milite pour positionner la capacité de réponse au plus près des organismes menacés.

3.1.3.2 Un accompagnement des ministères financé par des crédits exceptionnels

Pour relayer son soutien aux ministères, l'ANSSI accompagne depuis 2021, grâce aux crédits du plan France Relance, l'émergence et la structuration d'équipes de réponse à incident de sécurité informatique ou *Computer Security Incident Response Team* (CSIRT)[95], afin qu'ils traitent les incidents de cybersécurité de leur périmètre. À cette fin, l'ANSSI a mis en place un projet dénommé TEMPO. À partir de janvier 2022, les ministères volontaires ont pu rejoindre le projet et bénéficier de l'accompagnement proposé par l'ANSSI.

Les quatre phases du projet TEMPO

- phase I : le diagnostic de maturité par un prestataire permettant l'attribution d'un niveau à atteindre par le ministère dans la construction ou le renforcement de son CSIRT (88 000€ de janvier à avril 2022) ;
- phase II : la révision et l'adaptation de la feuille de route en un plan d'action échelonné et détaillé (mobilisation

[95] Les services usuellement portés par un CSIRT, notamment dans les groupes privés, sont : prise en compte de signalements d'attaque de la part de victimes potentielles, accompagnement de victimes dans le traitement de leurs incidents (gestion de crise, coordination de prestataires, accompagnement aux démarches légales et administratives), veille sur les vulnérabilités de produits majeurs pour leurs bénéficiaires, fourniture de services d'audit de sécurité, activités de sensibilisation et de formation.

du personnel de l'ANSSI) ;
- phase III : la mise en œuvre du plan d'action grâce à l'accompagnement d'un prestataire. Une durée d'environ un an est prévue pour cet accompagnement (2,7 M€ maximum de fin 2022 à décembre 2024) ;
- phase IV : « l'incubation » des CSIRT ministériels : de janvier à avril 2024, leurs agents sont appelés à suivre un parcours personnalisé de 65 ateliers pour une durée totale de 42 heures.

Dans ce cadre, l'ANSSI a aidé à la construction et la montée en maturité de dix CSIRT ministériels dont quatre sont à ce jour considérés comme pleinement opérationnels.

La démarche de mise en œuvre des CSIRT ministériels est trop récente pour qu'il soit possible d'en mesurer les performances. Les conditions de réussite de la construction et du renforcement des CSIRT ministériels reposent sur la capacité des ministères à prendre le relais du plan TEMPO et à garantir l'affectation sur le long terme des ressources humaines et financières nécessaires pour assurer la montée en maturité des CSIRT ministériels après le plan de relance.

Alors que l'ANSSI doit encore mettre en place les conventions qui permettront d'encadrer les relations entre le CERT-FR et les CSIRT ministériels, la question du financement courant de ces derniers devra être traitée.

3.1.3.3 Des équipes de réponses aux incidents sectoriels à mieux articuler avec les centres ministériels émergents

Des équipes de réponses aux incidents (CSIRT) ont été créés dans un certain nombre de secteurs d'activité en France. Le premier dès 1995 a été le CERT RENATER pour assister ses bénéficiaires, au sein de la communauté éducation-recherche française, en matière de sécurité informatique, notamment dans le domaine de la prévention, de la détection et de la résolution d'incidents de sécurité. Il permet l'acheminement rapide d'une communication vers les personnes appropriées sur les sites connectés au réseau RENATER.

Les CSIRT sectoriels remplissent des fonctions diverses et ont des niveaux de maturité très différents.

Le CERT Santé évolue dans un cadre légal défini par le code de la santé publique et plusieurs arrêtés publiés depuis 2015. C'est une structure nationale d'assistance apportant un appui aux agences régionales de santé (ARS) ainsi qu'aux établissements de santé, aux organismes et services exerçant des activités de prévention, de diagnostic ou de soins, ainsi qu'aux établissements et services médico-sociaux. Ses trois principales missions, assurées en 24/24 et 7/7, sont la réponse à incidents, la veille proactive relative aux vulnérabilités et la réalisation d'audits et de bulletins de sécurité. Ce CSIRT démontre une forte maturité, selon l'ANSSI, et les incidents[96] les plus importants sont gérés, ou *a minima* coordonnés, par lui, sans intervention du CERT-FR. Une comitologie dédiée permet une synchronisation deux fois par mois sur ces aspects opérationnels entre les deux entités.

[96] 581 incidents ont été déclarés au CERT Santé en 2023 dont 163 ont donné lieu à des demandes d'accompagnement et 93 à des interventions d'appui technique (investigations numériques et aide à la remédiation).

Le CSIRT Maritime, destiné aux entités publiques et privées du secteur maritime et portuaire, n'a pas pour fonction de procéder à la partie technique de la réponse à incident ni à la phase de remédiation. Sa mission principale est d'accompagner ses bénéficiaires à mettre en œuvre des mesures proactives pour réduire les risques d'incidents de sécurité informatique. Il porte également conseil à ses bénéficiaires sur les bonnes pratiques et les réactions à avoir lorsque ces incidents se produisent.

Le CSIRT CNES est une structure interne du centre national d'études spatiales. Son périmètre d'activité couvre l'ensemble des centres du CNES et plus globalement l'ensemble de la communauté cyber du CNES. Son rôle recouvre le traitement de tous les incidents ayant trait à l'espionnage et à la fuite de données ainsi que la détection des menaces et la prévention des cyberattaques en améliorant la prise de conscience et la résilience en cybersécurité.

La DINUM, au titre de la mise en œuvre de l'IGI 1337, dispose d'un CSIRT pour les produits numériques interministériels, opérationnel depuis septembre 2024.

Le périmètre d'intervention de ces CSIRT est un sujet qui nécessite encore d'être précisé. Le CSIRT CNES, par exemple, a vocation à étendre tout ou partie de ses services à l'ensemble du secteur spatial.

L'articulation doit également être pensée avec les CSIRT ministériels, déployés pour beaucoup grâce au programme TEMPO, financé par le plan de relance de 2021 (cf. *supra*). Pour certains, elle est assez naturelle du fait de leur positionnement.

Ainsi, le CERT Aviation France est une association[97] qui fournit des services de traitement de premier niveau de réponse aux incidents ainsi qu'une veille sur les vulnérabilités informatiques. Il effectue également des sensibilisations auprès de ses bénéficiaires et se coordonne avec les acteurs régionaux et nationaux de la cybersécurité. Rattaché à la direction générale de l'aviation civile, ce CERT entretient des liens étroits avec le ministère de la transition écologique et de la cohésion des territoires (MTECT). La création du CSIRT Écologie (CSIRT du MTECT) au travers du projet TEMPO instaure un nouveau lien opérationnel entre CSIRT ministériel et CSIRT sectoriel.

Le CERT des entreprises de défense, nommé CERT-ED, a pour bénéficiaires les entreprises de la base industrielle et technologique de défense. Il est rattaché à la direction du renseignement et de la sécurité de la défense (DRSD). Le CERT-ED partage ses connaissances et son expérience en sensibilisant ses bénéficiaires, contribue à réduire le risque aux attaques informatiques en fournissant sur demande ou préventivement des avis sur les vulnérabilités logicielles ou matérielles, accompagne les victimes d'incidents de sécurité, et se coordonne et coopère avec les acteurs régionaux et nationaux de la cybersécurité.

Pour d'autres, l'articulation est encore à affiner.

C'est le cas pour le CERT Social, qui est porté par la caisse nationale de l'assurance maladie (CNAM). Plus récent que le CERT Santé, il couvre les besoins internes des organismes de la CNAM, de la caisse nationale des allocations familiales, de la caisse nationale d'assurance vieillesse, de l'agence centrale des organismes de sécurité sociale et de la mutuelle sociale agricole. Il est également un interlocuteur fédérateur des organismes des secteurs publics santé et social en assurant, en heures ouvrées, plusieurs types de missions : faciliter le partage de

[97] Les membres fondateurs de cette association sont Air France, le groupe ADP, Dassault Aviation, la DGAC (Direction Générale de l'Aviation Civile), la FNAM (Fédération Nationale de l'Aviation et de ses Métiers), Thalès AVS, et l'UAF (Union des Aéroports français et Francophones Associés).

l'information et la coordination afin d'empêcher ou de limiter les cyberattaques pouvant impacter les organismes de son périmètre, mutualiser des capacités de défense et de prévention contre des incidents, informer et sensibiliser concernant les attaques. Le CERT Santé et le CERT Social sont des CSIRT sectoriels qui coexistent sur un périmètre d'applicabilité très proche de celui du CSIRT des ministères sociaux. Des projets d'échanges entre ces trois CSIRT sont en cours pour renforcer le niveau de maturité cyber de ce secteur et optimiser le suivi et la coordination de traitement des incidents sur les entités de ce périmètre.

3.1.3.4 Des centres de réponse aux incidents régionaux, dont l'articulation avec les autres dispositifs et le financement restent à élaborer

Depuis 2021, et toujours grâce au plan France Relance, l'ANSSI accompagne l'émergence et la structuration de 14 CSIRT territoriaux dont deux en outre-mer. Toutes les régions, à l'exception de la région Auvergne Rhône-Alpes, ont procédé à la signature, entre septembre 2021 et avril 2022, de conventions avec le SGDSN. Ces conventions définissent le périmètre couvert par les CSIRT régionaux (PME, ETI, collectivités territoriales et établissements publics associés, associations nationales), la composition minimale d'une équipe de réponse aux incidents, et les services minimums à fournir à destination des bénéficiaires.

Services minimums

Proposer gratuitement les services suivants en jours ouvrés :

- mise en œuvre d'une plateforme téléphonique et des moyens informatiques nécessaires à la réception des demandes relatives à des incidents informatiques ;
- qualification et triage des incidents ;
- suivi des incidents ;
- mise en relation avec des prestataires labellisés ExpertCyber ou qualifiés par l'ANSSI ;
- information et conseil relatifs aux poursuites juridictionnelles ;
- référencement des prestataires locaux labellisés et qualifiés en cohérence avec l'ANSSI et Cybermalveillance.gouv.fr ;
- relais et transfert des informations pertinentes vers le CERT-FR, Cybermalveillance.gouv.fr, les autres CSIRT et l'Intercert-FR ;
- consolidation de l'incidentologie régionale et partage du résultat avec le CERT-FR.

En contrepartie, chaque CSIRT régional bénéficie d'une subvention unique d'un montant d'un million d'euros par région pour la durée de trois ans de la convention, de la participation à un parcours d'incubation, et d'un appui pour rejoindre l'association InterCERT-France[98].

Dans la pratique, la création de ces centres a pris des formes très différentes : en Île-de-France, le pôle « transformation numérique » des services administratifs de la région a passé convention avec un prestataire de service pour répondre aux incidents. Dans le Grand-Est comme en Occitanie et en Nouvelle-Aquitaine, ce sont des associations qui sont chargées d'assumer le rôle de CSIRT. En Grand-Est comme en Occitanie, ces associations sont

[98] En outre-mer, un nombre insuffisant de prestataires de réponse à incident ayant été identifié, l'ANSSI a proposé aux exécutifs régionaux de soutenir dans le cadre du plan France Relance la création de centres de ressources cyber. Dans ce cadre, des contributions financières ont été accordées à trois centres en création : Guadeloupe-Guyane-Saint-Barthélémy (1 M€), Réunion (0,6 M€), et Nouvelle-Calédonie (0,4 M€).

spécialisées dans l'aide aux acteurs économiques régionaux, En Nouvelle-Aquitaine, l'association a un tropisme cyber puisqu'elle gère également le campus cyber territorial (voir *infra*).

Les services fournis par les CSIRT varient d'une région à une autre, en fonction de la maturité des bénéficiaires et des partenaires identifiés, les écosystèmes étant de fait très différents.

Le caractère très récent de ces CSIRT explique leur faible notoriété - et ne permet pas d'évaluer leur performance. Le volume des incidents signalés et traités est encore faible et la région Île-de-France a demandé au prestataire chargé de répondre aux appels de profiter de ses disponibilités pour assurer la promotion du dispositif auprès des bénéficiaires potentiels. Le développement de relations de confiance avec suffisamment de prestataires expérimentés pour accompagner leurs bénéficiaires est également un défi, notamment dans les régions où les entreprises du numérique sont peu implantées. L'Île-de-France est, de ce point de vue, extrêmement mature alors que la Corse et les territoires ultramarins apparaissent démunis.

Les financements du SGDSN pour la mise en place des CSIRT ministériels et régionaux sont d'une durée limitée à trois ans. À l'issue, le relais devrait être pris par les régions (la région Île-de-France verse déjà 1,6 M€ en complément du million accordé par l'État) pour assurer la pérennité des CSIRT ou un modèle économique mêlant financeurs publics et bénéficiaires – ou leurs représentants – devra être établi. Les réflexions en la matière mériteraient d'être accélérées.

Recommandation n°3. (SGDSN, ANSSI) Définir l'articulation entre les CSIRT ministériels, sectoriels et territoriaux et s'assurer de la pérennité de leur financement.

3.1.4 La nécessité d'une observation centralisée de la menace cyber

L'analyse de la menace est, à ce jour, extrêmement diffuse et ces multiples observations produisent une vision segmentée et manquent de consolidation. La fonction doit être mieux investie pour asseoir une politique solide de lutte contre les cybermenaces.

3.1.4.1 Une observation diffuse et parcellaire

En France, dès sa création en 2009 et progressivement avec la catégorisation des opérateurs d'importance vitale puis des opérateurs de service essentiels, l'ANSSI présente, dans ses rapports d'activité, une analyse de la menace qui pèse sur les systèmes d'information de ces entités du haut du spectre. Depuis 2021, elle édite une synthèse de menaces cyber observées à partir de multiples sources d'informations – celles issues de sa pratique de conseil et d'assistance mais aussi sources ouvertes, partenaires internationaux et nationaux, victimes, etc.

Le centre de réponse aux incidents de l'ANSSI, CERT-FR, outre ses actions de cyberdéfense, tire du suivi de cet état général de la cybermenace, des publications ponctuelles

sous forme de guides et notes techniques[99], des synthèses thématiques à destination d'organismes estimés menacés (collectivités territoriales[100], secteur des télécommunications[101]), des bulletins d'actualités précisant les vulnérabilités et expositions (*i.e.* failles de sécurité) identifiées dans un système d'information[102], et des évaluations de la menace pour la préparation de grands événements à portée internationale sur le territoire national[103], comme la coupe du monde de rugby en 2023 et les Jeux olympiques et paralympiques de Paris 2024, dans lesquels l'ANSSI est partie prenante en tant qu'autorité nationale de régulation.

À ces publications nationales, s'ajoutent celle, au niveau européen, de l'ENISA, qui a publié le 19 octobre 2023 la 11ème édition de son panorama de la menace, rapport annuel sur l'état des cybermenaces en Europe, et le panorama de la cybercriminalité (*Internet Organised Crime Threat Assesment* – IOCTA) produit également chaque année par Europol.

Créé en 2017 pour répondre aux demandes d'information et d'assistance de la part de particuliers, de petites entreprises ou de collectivités, face à la recrudescence des arnaques en lignes et autres actes de malveillance numérique, le groupement d'intérêt public d'assistance aux victimes d'actes de cybermalveillance (GIP Acyma) consacre, depuis 2019, un chapitre à l'observation de la menace numérique dans son rapport annuel d'activité. Cette mission « d'observation » qui figure dans son arrêté de création (cf. *supra*) lui confie même un rôle de préfiguration d'un observatoire dédié[104]. Le GIP a ainsi lancé au second semestre 2019 un groupe de travail interne pour élaborer des propositions sur le périmètre, l'organisation et les moyens nécessaires à la constitution de ce futur observatoire. Les conclusions sont restées sans suites.

Des « états de la menace liée au numérique » ont été établis par l'ensemble des services du ministère de l'intérieur, sous la coordination de la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC[105]) de 2017 à 2019. Il relève désormais, du commandement du ministère de l'intérieur dans le cyberespace (COMCYBER-MI)[106] de produire chaque année un rapport sur la cybercriminalité pour le compte de l'ensemble des services du ministère de l'intérieur. Le premier rapport date de 2024 et porte sur l'année 2023. Il s'inscrit « *en complémentarité avec les analyses annuelles de l'ANSSI* », bénéficie des

---

[99] Comprendre et anticiper les attaques DDoS, 20 mars 2015, https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos ; Les dénis de service distribués (DDoS), 5 septembre 2023, https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos

[100] Synthèse de la menace ciblant les collectivités territoriales, 23 octobre 2023, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-008.pdf

[101] État de la menace ciblant le secteur des télécommunications, 18 décembre 2023, https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/

[102] Bulletin d'actualité du 20 décembre 2021, https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-053/ Bulletin d'actualité du 6 novembre 2023, https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-048/

[103] Grands évènements sportifs – Évaluation de la menace 2023, 30 août 2023, https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-005/

[104] « *Le Groupement a pour objet d'assurer : […] la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.* »

[105] Devenue DPSIS en 2020, puis transformée en direction des entreprises et partenariats de sécurité et des armes (DEPSA) en 2023 dans le cadre de la réorganisation du ministère de l'intérieur (Cf. Décret n° 2023-582 du 5 juillet 2023 modifiant le décret no 2013-728 du 12 août 2013 modifié portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer).

[106] Cf. décret n°2023-1084 du 23 novembre 2023. Le COMCYBER-MI (…) a pour mission : (…) - de produire chaque année un rapport d'état de la menace cyber du ministère de l'intérieur ; (…).

travaux du CEntre d'analyse et de regroupement des Cybermenaces (CECyber) du COMCYBER-MI et repose aussi sur les données du service statistique ministériel de la sécurité intérieure (SSMSI), complétées par d'autres sources institutionnelles.

Ces données recouvrent un ensemble d'infractions susceptibles d'être commises ou facilitées par l'utilisation d'un système informatique, généralement connecté à un réseau. Elles prennent ainsi en compte :

- les infractions liées aux systèmes d'information et aux systèmes de traitement automatisé des données (STAD) ayant pour origine le développement des réseaux informatiques et notamment internet (accès frauduleux dans un STAD, altération d'un système, attaque par déni de service[107], etc.) ;
- les infractions liées aux formes de criminalités « traditionnelles », qui ont pu évoluer avec les nouvelles technologies de l'information et de la communication (NTIC) ou être facilitées par ces dernières : usages frauduleux de cartes de crédit en ligne, hameçonnage[108], menaces et injures de toute nature ou images pédopornographiques diffusées via les nouveaux moyens de communication électronique, etc.

Pour ces dernières, leur caractérisation cybercriminelle dépend de l'appréciation des services opérationnels de la police et de la gendarmerie, ce qui crée une relative incertitude sur leur caractère exhaustif comme sur leur justesse. L'aide au remplissage de ces informations demande à être renforcée. En outre, selon le ministère de l'intérieur, les cyberattaques ne donneraient lieu qu'à une plainte déposée pour plus de 205 faits constatés, limitant ainsi les données exploitables au plan statistique. La situation devrait s'améliorer progressivement avec la mise en œuvre opérationnelle du « 17 Cyber » (cf. *infra*) depuis le 17 décembre 2024.

Par ailleurs, les chiffres sur les incidents cyber sont souvent avancés par des acteurs privés qui proposent des solutions de sécurité. Selon l'ANSSI, ils sont très peu sourcés et pourraient être surévalués dans le but commercial d'augmenter la vente de solutions techniques. Lorsqu'ils sont produits par des acteurs publics ou privés qui interviennent dans la réponse à incident ou dans l'assistance aux victimes, leur périmètre est souvent restreint à un type de victimes, une famille de sinistre ou un mode d'intervention. En outre, ils sont souvent essentiellement représentatifs de la capacité de l'observateur à traiter les évènements qui lui sont signalés et donc partiels.

L'enjeu est donc de structurer l'observation de la menace, à partir des multiples sources d'informations existantes mais avec un prisme et des méthodes scientifiques d'analyse de données qui lui confèrent une légitimité incontestable. C'est le préalable indispensable à l'établissement des cartographies des attaques, à la construction d'une véritable prévention des risques cyber et d'une protection robuste des systèmes d'information, et, ainsi, à l'adaptation de l'offre d'assistance[109].

---

[107] Vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à saturation ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service, à l'aide d'un ordinateur.

[108] L'hameçonnage ou phishing est un SMS ou mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance.

[109] Les six catégories de missions de la cyberdéfense française sont : la prévention, l'anticipation, la protection, la détection, l'attribution et la réaction (remédiation, répression des infractions et actions militaires) ; *source Revue stratégique de cyberdéfense 2018, SGDSN*.

3.1.4.2 Un observatoire de la menace à mettre en œuvre au niveau interministériel

Deux leviers supplémentaires de collecte des informations sur les cyberattaques ont été établis récemment : la directive (UE) 2022/2555, relative à la cybersécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union européenne, dite directive NIS 2, étend le périmètre des organismes régulés et leur impose le signalement des incidents de cybersécurité ; la loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) de 2023 fait obligation aux personnes morales et physiques, victimes d'attaques informatiques malveillantes dans le cadre de leur activité professionnelle, de porter plainte pour préserver leur droit à indemnisation au titre de leur contrat d'assurance. Pour autant, une méthode de décompte normalisée des cyberattaques, tenant compte de leur intensité et de leur profondeur, reste à définir, afin de disposer d'une base de données fiable.

L'ANSSI constate que des projets visant à construire un modèle de données relatives aux incidents cyber, à centraliser les informations et à produire des statistiques sont déjà en cours dans différents secteurs (la réponse à incident, le traitement judiciaire des plaintes, les assurances, …), dans un processus entrepreneurial d'amélioration de leur activité. Mais leur caractère parcellaire et la multiplication des organismes concernés engagent à centraliser la fonction d'observation. C'est ce qui a conduit l'ANSSI, autorité nationale et seule récipiendaire des notifications d'incidents prévues par la loi, à la reprendre au GIP Acyma.

À ce stade, compte tenu de ses priorités, l'ANSSI a seulement ébauché une étude sur le sujet en 2023 qui induit un accroissement de ses ressources. Deux options sont ouvertes :

- centraliser les résultats des études réalisées par les organismes privés et publics pour produire, à moindre coût, des statistiques plus riches ;
- enrichir cette veille par la conduite d'enquêtes de victimation, sur le degré de maturité cyber des organismes ou le niveau de résilience cyber des différents publics.

Le second scénario plus ambitieux permettrait de fournir des clés pertinentes pour orienter et évaluer les politiques publiques dans la prévention des incidents cyber et pour l'assistance apportée aux victimes.

En tout état de cause, la centralisation de la fonction d'observation au niveau interministériel s'impose et l'ANSSI, « *autorité nationale de la défense et de la sécurité des systèmes d'information »* et acteur de confiance pour les parties prenantes qui fourniront des données, paraît la mieux qualifiée pour l'assumer.

Il est désormais nécessaire de fixer l'organisation de l'activité en déterminant les conditions de recueil des informations et notamment des déclarations d'incidents et des infractions. De même, il convient de s'interroger sur la fréquence des enquêtes complémentaires à mener et sur les partenariats à établir avec les organismes de recherche existants, pour réaliser les études transversales et qualitatives susceptibles d'enrichir l'observation des cybermenaces. La question du partage d'informations avec certains partenaires étrangers, par exemple au sein de l'Union européenne et de l'OTAN (à l'instar des productions de la division « analyse » du *National Cyber Security Centre* (NCSC) britannique) pourrait être également posée dans ce cadre.

Dans les observations définitives relatives au contrôle de l'ANSSI (septembre 2022), la Cour recommandait au SGDSN et à l'ANSSI de « *mettre en place rapidement l'observatoire de la menace cyber, en fixer les objectifs, la répartition des responsabilités et les modalités de*

fonctionnement ». La Cour réitère cette recommandation visant à mettre en place une fonction d'observation au niveau interministériel.

Recommandation n°4. (SGDSN, ANSSI) Mettre en place à court terme un observatoire de la cybermenace au sein de l'ANSSI, centralisant à l'échelle nationale les données et les analyses, afin d'en prévoir l'évolution et les moyens de la prévenir et de la contrer.

3.1.5 Une fonction de contrôle qui doit changer de dimension

L'ANSSI, en sa qualité d'autorité nationale de sécurité et de défense des systèmes d'information, accompagne les entités régulées dans la sécurisation de leur système d'information et réalise des audits afin de vérifier son effectivité et ses performances. Si elle dispose déjà de la capacité à imposer des sanctions administratives, cette dimension doit être plus fortement structurée, afin de garantir une exécution efficace des obligations réglementaires de cybersécurité.

3.1.5.1 Une capacité d'audit limitée de l'ANSSI malgré une plus grande souplesse de la programmation

Les audits sont réalisés dans différents cadres : homologation, évaluation avant mise en production, contrôle règlementaire, etc.

Au total, 137 audits ont été réalisés par l'ANSSI depuis 2020 : 14 en 2020 ; 27 en 2021 ; 20 en 2022 ; 34 en 2023 ; 32 en 2024[110] et 10 à date d'avril 2025 ; soit une moyenne de près de 23 contrôles par an.

Tableau n° 9 : Répartition de l'activité de contrôle 2020-2024 par type de bénéficiaires

Statut	Nombre d'organismes	Part	Nombre de contrôles	Part	Moyenne des contrôles par organisme
Europe	1	2,3%	1	1,0%	1,0
État	9	20,9%	35	34,3%	3,9
Établissements publics	9	20,9%	19	18,6%	2,1
Collectivités locales	1	2,3%	4	3,9%	4,0
Privé non lucratif	1	2,3%	1	1,0%	1,0
Privé	22	51,2%	42	41,2%	1,9
Total	43	100,0%	102	100,0%	2,4

Source : ANSSI

[110] À noter que des créneaux d'audit ont été suspendus pendant la période des Jeux olympiques et paralympiques de Paris 2024 afin de préserver la capacité de remédiation en cas d'urgence, qui relève de la même équipe.

Le spectre des audits est large, avec un équilibre global entre secteur public (46,5 % des organismes, 57,8 % des audits) et secteur privé (53,5 % des organismes, 42,2 % des audits). Les audits menés sur les organismes privés sont plus diffus, alors que les entités publiques sont plus souvent auditées.

Les capacités d'audit du bureau qui en est chargé au sein de la sous-direction des opérations de l'ANSSI ne permettent pas de suivre la croissance significative des demandes. À titre d'exemple, pour l'exercice 2019, 68 demandes d'audit prioritaires ont été remontées en comité de pilotage des audits, pour une capacité d'audits de 46. À ces demandes, validées en comité de pilotage, s'ajoutent les demandes exceptionnelles liées aux grands évènements.

En 2019, une réflexion a été engagée, visant à l'externalisation des audits. Le champ d'application a exclu les prestations associées à des missions régaliennes[111], le contrôle de points d'importance vitale, le contrôle des opérateurs télécom, les audits réalisés au titre du code pénal. Une ligne budgétaire de 200 000 euros a été inscrite à l'exercice 2019, représentant quatre à cinq prestations d'audit. L'ANSSI s'est initialement appuyée sur le marché de conseil, d'expertise et d'audit du ministère de l'agriculture, puis sur un accord-cadre passé, en 2022, par le secrétariat général du ministère de l'économie, des finances et de la souveraineté industrielle et numérique qui permet notamment l'accès à des prestations d'audit en sécurité des systèmes d'information[112].

La définition restrictive du périmètre d'externalisation explique pour partie que seuls deux audits ont été externalisés en 2023.

La planification des audits est régie par le processus « P12 » de fonctionnement de l'ANSSI – « réaliser des audits, inspections et contrôles » -, créé fin 2014. Annuelle, elle était préparée à l'automne de l'année précédente, par le croisement des demandes des organismes régulés – spontanées ou induites, notamment par les coordinateurs sectoriels de l'ANSSI (cf. *infra*), et des disponibilités[113] du bureau audits en sécurité de la sous-direction des opérations.

L'amplification des retards et l'annulation de nombreux audits au cours de la période contrôlée par la Cour résultent de plusieurs facteurs : l'établissement d'une convention d'audits peut être laborieuse (parfois plus d'un an) du fait de désaccord sur les dates de réalisation ou sur les conditions pratiques d'évaluation des scénarios de menace à évaluer et / ou de

[111] En particulier les services du président de la République et du Premier ministre, les services de renseignement, les inspections ministérielles, les demandes d'autorisation au titre de l'article R 226 du code pénal (pour la fabrication, l'importation, l'acquisition, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques listés en annexe de l'arrêté du 4 juillet 2012 , notamment ceux conçus pour réaliser l'interception, l'écoute, l'analyse, la retransmission, l'enregistrement ou le traitement de correspondances émises, transmises ou reçues sur des réseaux de communications électroniques), les contrôles opérateurs télécom ainsi que les contrôles de PIV. En revanche, peuvent être externalisés les contrôles des SI d'importance vitale et les audits d'homologation FR, OTAN et UE jusqu'à un certain niveau de criticité. Pour les audits OTAN et UE, une convention spécifique doit être passée avec le prestataire, afin de préciser dans une annexe de sécurité les modalités de traitement des informations classifiées.

[112] Cet accord donne également accès à des prestations de réponse aux incidents de sécurité et prestations qualifiées (PRIS) et à des prestations de certification de sécurité de premier niveau (CSPN) de produits informatiques (logiciels) réalisées par des centres agréés par l'ANSSI (Centres d'évaluation de la sécurité des technologies de l'information – CESTI).

[113] Le bureau audits en sécurité de l'ANSSI (SDO/DCA/AES) présente sa capacité d'audit prévisionnelle sous forme de « tickets ». Un ticket d'audit représente environ 45 jours par ticket pour la préparation et l'accompagnement préalable, la réalisation de l'audit et la rédaction du rapport. Certaines entités bénéficient d'une « garantie » d'audits, des « tickets » leur étant réservés annuellement pour répondre à leurs éventuelles demandes.

l'impréparation des équipes d'exploitation du périmètre d'audit chez les bénéficiaires, voire de leur réticence, notamment dans les cas de contrôle réglementaire. Les perturbations apportées au calendrier de programmation déterminé annuellement ne permettaient pas de réaffecter les vacations libérées à d'autres sujets de contrôles.

Les ressources humaines constituent aussi un point sensible. Les personnes chargées de l'audit interviennent dans les opérations de défense et cette double fonction est à la fois le gage de leur expertise et une souplesse de l'organisation de l'activité. Elles acquièrent ainsi une forte visibilité sur leur marché du travail qui en font des cibles de démarchages, notamment de la part du secteur privé, tout en complexifiant les recrutements pour l'ANSSI du fait du niveau d'expertise requis pour occuper ces postes. Les départs enregistrés en 2021 et 2022 n'ont pas été compensés par les recrutements de même ampleur et l'effectif des auditeurs techniques est passé de 19 en septembre 2020, à 15 en septembre 2021 et à 14 en septembre 2022.

Pour fluidifier le processus, laisser place à l'acceptation de demandes d'audit inopinées, et s'adapter aux contraintes opérationnelles de l'ANSSI ou des bénéficiaires, une nouvelle procédure de planification des audits « en continu » a été établie en organisant des arbitrages plus fréquents de sorte à ajuster les priorités des audits. En contrepartie, un compte rendu mensuel est diffusé en interne, affichant un planning prévisionnel des interventions à quatre mois[114] et identifiant la disponibilité des équipes d'audits, pour donner une meilleure visibilité aux différents relais internes des besoins d'audits.

À cet égard, le rôle des délégués sectoriels de l'ANSSI – rattachés à la sous-direction de la stratégie (SDS) et chargés de coordonner les relations et les actions de l'ANSSI auprès des administrations et opérateurs publics et privés – est déterminant pour définir les demandes et pour assurer la préparation des prestations d'audit, conjointement avec le bureau en charge de les réaliser et les bénéficiaires. En effet, comme l'analyse des reports et annulations le démontre, la phase de cadrage de l'audit est particulièrement sensible et la note d'amélioration de la procédure propose l'établissement de critères pour déterminer l'entrée en phase de réalisation. En réalité, il s'agit moins de définir des critères que d'établir une procédure permettant de définir avec le « bénéficiaire » le périmètre et le calendrier de réalisation de l'audit.

Cette planification glissante gagnerait à être établie à partir d'une véritable cartographie des risques réalisée, de manière plus formalisée qu'actuellement, par ces délégués sectoriels en collaboration avec les responsables des organismes régulés et les autres acteurs de l'ANSSI. Cette cartographie des risques, établie de manière contradictoire, permettrait d'engager la responsabilité des dirigeants des organismes régulés et de faciliter ainsi la conduite des audits, grâce à une meilleure mobilisation des équipes d'accueil.

Cette démarche est éloignée de la posture de la sous-direction des opérations de l'ANSSI qui valorise davantage la relation de confiance avec les organismes audités. Celle-ci est particulièrement soulignée vis-à-vis des opérateurs privés, pour les engager à dépasser la notion de secret industriel et commercial et leur réticence à dévoiler les défaillances de leur système d'information. L'ANSSI considère que cette relation de confiance lui confère une meilleure

[114] Le concept de « ticket » est ainsi remplacé par « la charge d'audit courante », *i.e.* l'identification de la capacité d'audit du bureau concerné, tenant compte de la quantité de prestations en cours de réalisation et de la charge prévisionnelle, basée sur la planification des audits anticipée sur le trimestre glissant suivant le mois en cours.

connaissance - et donc maîtrise - des vulnérabilités des organismes. La démarche d'audit s'inscrit, de ce fait, dans la continuité de l'assistance technique offerte par ailleurs par l'ANSSI.

Cette posture explique pour partie l'absence de sanctions appliquées aux OIV et OSE, pourtant prévues par les lois de programmation de 2013 et de transposition de NIS 1 de 2018 (cf. *supra*).

Sanctions définies dans NIS 1 et transposées en droit français

Pour les OIV, l'article L. 1332-7 du code de la défense sanctionne d'une amende de 150 000 euros le fait, pour les dirigeants, d'omettre, après une mise en demeure, d'établir un plan de protection ou de réaliser les travaux prévus et d'entretenir en bon état les dispositifs de protection antérieurement établis. Le même article prévoit une amende plus lourde encore pour « *les personnes morales déclarées responsables des mêmes infractions* » en renvoyant aux articles L. 121-2 et L. 131-38 du code pénal.

Pour les OSE, la loi de 2018 prévoit différents niveaux de sanctions pour les dirigeants : lorsqu'ils ne satisfont pas aux obligations de déclaration d'incident ou d'information du public (75 000 € 50 000 € pour les FSN) ; lorsqu'ils ne se conforment pas aux mesures de sécurité (100 000 €,75 000 € pour les FSN) ; lorsqu'ils font obstacle aux opérations de contrôle (125 000 €, 100 000 € pour les FSN).

Elle explique également la portée relativement faible de ces audits en termes d'exemplarité, faute de communication sur leurs résultats. Il convient également de noter que les audits réalisés portent sur un ou plusieurs systèmes d'information et permettent difficilement, de ce fait, d'apprécier la sécurisation d'ensemble des organismes.

3.1.5.2 Une intensification et une priorisation nécessaire des contrôles

Cette posture est désormais difficilement tenable, dès lors que la directive européenne NIS 2 met l'accent sur la capacité des États à imposer des mesures - et notamment des amendes administratives - en cas de violation des règles de gestion des risques en matière de cybersécurité et des obligations d'information qui s'imposent aux organismes régulés (cf. paragraphe 127 de la directive NIS 2).

La transposition de la directive NIS 2 en droit français a défini une nouvelle organisation en matière de contrôle. Elle consiste à mettre en place une commission des sanctions, rattachée au SGDSN, et offrant des garanties d'impartialité, qui statuera sur les décisions individuelles de sanction sur la base d'une procédure contradictoire.

Par ailleurs, l'ANSSI prévoit de créer en son sein une distinction claire entre ses missions d'accompagnement et d'assistance d'une part, de contrôle d'autre part, afin de maintenir le rapport de confiance avec ses bénéficiaires et d'inscrire le contrôle en complémentarité avec ses missions historiques. L'ANSSI travaille donc son organisation interne pour assurer le cloisonnement des informations qui seraient communiquées par des bénéficiaires à l'occasion d'un accompagnement ou d'une assistance pour le traitement d'un incident de sécurité sur ses systèmes d'information.

Si la confiance est certainement un élément capital pour maintenir la capacité à assister les organismes, un équilibre doit cependant être trouvé avec l'impératif d'efficacité des contrôles, compte tenu des enjeux de coûts et d'activité représentés par les cyberattaques mais également des ressources humaines nécessaires pour mener à bien ces contrôles.

En pratique, c'est moins l'étanchéité des structures qui doit être recherchée que la construction d'un dispositif gradué permettant, en cas d'identification d'une non-conformité, d'enjoindre aux responsables de l'entité concernée de mettre en place les mesures adaptées et, éventuellement de recourir à des services d'accompagnement et de soutien désignés, avant d'imposer une sanction, au nombre desquelles la directive européenne compte l'imposition d'une « *suspension temporaire d'une certification ou d'une autorisation concernant tout ou partie des services concernés fournis ou des activités menées par une entité essentielle et […] une interdiction temporaire de l'exercice de fonctions de direction par une personne physique à un niveau de directeur général ou de représentant légal* ».

Par ailleurs, compte tenu de l'élargissement considérable de l'activité de contrôle au regard du nombre d'entités concernées dans les secteurs régulés par la directive NIS 2, le positionnement de l'ANSSI doit être reconsidéré. Le « passage à l'échelle » justifie de construire un dispositif de contrôle qui, tout en restant centralisé à l'ANSSI, permettrait d'appuyer la démarche sur les contrôles sectoriels – et les organismes qui en ont la charge – tels que celui existant pour les entités financières[115]. La mise en œuvre de tels leviers nécessiterait d'outiller les organismes de contrôle sectoriel sur les sujets de la cybersécurité.

Enfin, une réflexion devrait être menée sur la communication relative à ces contrôles de manière à en conforter la valeur d'exemplarité.

Recommandation n°5. (SGDSN, ANSSI) Établir une cartographie des risques à partir des résultats des mesures d'accompagnement et d'audits réalisés ; intensifier et prioriser les contrôles réalisés par l'ANSSI et les entités de contrôle sectorielles.

3.2 Une augmentation continue des moyens de l'ANSSI

3.2.1 Une entité omniprésente sur le champ de la sécurité des systèmes d'information civils

L'ANSSI est l'héritière d'une série d'organismes chargés d'assurer la sécurité des informations sensibles, notamment de l'État, qui débute avec la direction technique des chiffres (DTC), créée en 1943 à Alger et se prolonge jusqu'à la direction centrale de la sécurité des systèmes d'information (DCSSI) créée par le décret n° 2001-693 du 31 juillet 2001 au sein du secrétariat général de la défense nationale.

Le décret de 2009 modifié confère à l'ANSSI un champ de compétences bien plus large que la sécurité des systèmes d'information de l'État.

Elle est érigée en autorité nationale en matière de sécurité et de défense des systèmes d'information et, à ce titre, elle exerce également une mission de conseil et de soutien aux OIV

[115] Cette démarche garantirait, par ailleurs, une cohérence avec la mise en œuvre du règlement DORA (secteur bancaire), sous réserve d'une articulation à préciser entre les différentes autorités nationales.

et OSE ; elle contribue à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

Elle est le centre de réponse aux incidents de cybersécurité (CERT - *Computer Emergency Response Team*) gouvernemental et national français et l'expert français de cybersécurité dans les relations internationales. L'ANSSI participe à la sécurisation des systèmes d'information des organisations internationales dont la France est partie, en particulier pour assurer la protection des informations et supports classifiés. Outre les exercices nationaux et d'ampleur qu'elle anime à l'échelle nationale – par exemple pour préparer les jeux Olympiques et Paralympiques de 2024[116] -, l'ANSSI participe à certains exercices d'envergure internationale, menés à l'initiative des instances européennes et de pays alliés[117].

Sur le plan national, outre sa contribution essentielle à l'élaboration de normes, l'ANSSI, à l'instar de l'exercice de revue stratégique de cyberdéfense de 2018, a soutenu les travaux relatifs à l'élaboration de la stratégie nationale de cybersécurité de 2024. Elle est, de surcroît, chargée de la transposition de la directive européenne NIS 2. À l'autre bout du spectre, l'ANSSI mène des actions de sensibilisation aux enjeux de sécurité numérique auprès du grand public.

L'organisation française confie donc à l'ANSSI un rôle central et déterminant en matière de cybersécurité. Ce modèle tranche avec une organisation moins intégrée dans d'autres pays.

Ces multiples compétences justifient - voire nécessitent - le rattachement de l'ANSSI au SGDSN qui lui confère une dimension interministérielle. Celle-ci légitime son statut de service à compétence nationale (SCN) qui, malgré sa dénomination, n'a pas l'indépendance d'une agence.

Selon les États, un rattachement variable des entités en charge de la cybersécurité

Plusieurs États ont fait un choix identique à la France en positionnant leur agence de cybersécurité sous l'autorité du chef du gouvernement. C'est le cas de l'Italie (*Agenzia per la Cybersicurezza Nazionale* – ACN), la République tchèque (NUKIB) ou la Belgique (Centre de cybersécurité de Belgique).

D'autres pays privilégient un rattachement au ministère de la défense (Lituanie), aux services de renseignement (Royaume-Uni) ou un ministère à connotation plus économique (ministère des affaires économiques et de la transformation digitale en Espagne, ministère des affaires économiques et des communications en Estonie).

L'acteur central de la cybersécurité au Royaume-Uni est le National Cyber Security Centre (NCSC), créé en 2016 dans le cadre de la stratégie nationale de cybersécurité 2016-2021. Il exerce des fonctions proches de l'ANSSI, étant responsable de l'analyse de la menace, de la coordination et de la gestion des incidents. S'il établit des standards (CAF : *cyber assessment framework)* pour les ministères, il n'effectue pas d'audit. À côté du NCSC, a été créée fin 2020 une entité à vocation offensive, la National Cyber Force (NCF), en s'appuyant sur le personnel

[116] Exercice interministériel des 11 et 12 juillet 2023 visant à tester l'articulation entre la Cellule Interministérielle de Crise (CIC) du SGDSN et le Centre National de Commandement Stratégique (CNCS) des JO ; exercice JOP23 des 5 et 6 décembre 2023, participation à l'exercice Games Wide Paris 2024 JOP, 17 novembre 2023 organisé par Paris 2024 en préparation des Jeux Olympiques et Paralympiques ; REMPAR22 : en 2022, première initiative de l'ANSSI pour rassembler de multiples organisations et jouer en simultané un exercice de gestion de crise ; JOP Massifié : entraînement d'un nombre important d'opérateurs en lien avec les Jeux Olympiques et Paralympiques, de niveaux différents, par lequel chaque organisation avait l'opportunité de décliner un scénario de gestion de crise en fonction de son niveau de maturité, l'ANSSI assurant la mise à disposition du scénario, l'accompagnement et le suivi pour chaque organisation joueuse.

[117] Notamment EU-CyCLES, BlueOlex23, CySOPEx 23.

et les capacités du GCHQ (*Government Communications Headquarters*), en charge des services de renseignement. Ainsi, le modèle britannique, s'il confie à deux entités distinctes la stratégie défensive et la stratégie offensive, se caractérise par une plus grande intégration : le NCSC est en effet rattaché aux services de renseignement et la NCF est née du partenariat entre le ministère de la défense et les services de renseignement.

Aux États-Unis, le bureau du coordinateur national cyber (ONCD) et le Conseil à la sécurité nationale (NSC), positionnés auprès du président, coordonnent et orientent les politiques cyber. En outre, l'agence pour la sûreté des infrastructures critiques (CISA) a un rôle opérationnel et opère en parallèle d'une multitude d'agences sectorielles. Enfin, les départements de la justice et de la défense disposent d'entités dédiées à la cybersécurité, notamment en matière de réponse à incident et enquêtes.

L'Allemagne a fait le choix pour sa part de rattacher ses agences au ministère de l'intérieur. L'organisation allemande est relativement stable depuis la création, en 1991, de l'office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik* – BSI). Il est l'homologue naturel de l'ANSSI et exerce des missions proches. Contrairement à l'ANSSI, rattachée via le SGDSN aux services du Premier ministre, le BSI est rattaché au ministère de l'intérieur, et plus précisément la direction générale de la cybersécurité, qui relève du secrétaire d'État pour la sécurité des systèmes d'information. La direction générale est en charge de la stratégie allemande de cybersécurité et préside les instances dédiées. Au sein du BSI, une plateforme d'échanges opérationnels (*Nationales Cyber-Abwehrzentrum* – NCAZ) a pour objet de faciliter les relations entre les administrations susceptibles de contribuer au traitement des questions de cybersécurité. Son rôle est proche du C4 opérationnel existant en France. Dans ce cadre, le BSI constitue l'instance opérationnelle et concentre son action sur la défense et la sécurité des systèmes d'information.

3.2.2 Des moyens d'action réglementaires accrus

Dans le cadre de l'article 34 de la loi de programmation militaire (LPM) pour la période 2019-2024, l'ANSSI a pu, de manière circonstanciée, déployer des sondes dans les systèmes d'information de différents hébergeurs et transmettre des marqueurs d'attaques aux principaux opérateurs de communications électroniques (OCE). Toutefois, la portée de ce dispositif s'est avérée assez fortement limitée par les faibles capacités de détection des OCE et l'insuffisance de leur mobilisation[118], du fait de l'absence de caractère obligatoire et de la nécessité d'investissements à leur charge.

De ce fait, les articles 64 à 67 de la loi de programmation militaire 2024-2030 donnent à l'ANSSI de nouveaux moyens, en matière de sécurité des systèmes d'information, sous le contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) : mesures de filtrage de noms de domaine[119] en cas de menace contre la sécurité nationale ; communication de certaines données techniques de cache de serveurs de systèmes de noms de domaine ; obligation pour les éditeurs de logiciel victimes d'un incident informatique sur leurs systèmes d'information ou ayant une vulnérabilité critique

[118] À ce jour, seul un des OCE a traité les éléments transmis par l'ANSSI. Cet opérateur pourrait entrer dans un processus pérenne, avec une capacité potentielle de traitement allant jusqu'à 6 campagnes par an. En effet, cet OCE a injecté les marqueurs transmis dans son outil existant de protection contre les attaques par déni de service. Concernant les trois autres OCE, la réglementation ne revêtant pas un caractère contraignant, la situation évoluera après la mise en application de la nouvelle LPM.

[119] Le « Domain Name System » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine facile à retenir à une adresse IP (Internet Protocol) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 »). La maîtrise de ces DNS par des acteurs malveillants autorise de nombreuses attaques qui représentent la majorité des incidents traités par l'ANSSI.

sur un produit ou un service d'en informer l'ANSSI et leurs clients français ; renforcement des capacités de détection des cyberattaques et d'information des victimes.

Ces mesures devaient entrer en vigueur après publication des décrets d'application au plus tard au premier trimestre 2024. Ces textes ont été publiés en mai et juillet 2024[120]. Parallèlement, l'ANSSI a lancé le 29 janvier 2024 une consultation publique sur le projet de décret en Conseil d'État, de sorte à sensibiliser les hébergeurs, fournisseurs d'accès à internet (FAI), bureaux d'enregistrement de noms de domaine, éditeurs de logiciels et opérateurs de centres de données, qui sont les premiers concernés, à ces nouveaux dispositifs et à définir les modalités d'application de la manière la plus consensuelle possible.

3.2.3 Une organisation évolutive et une croissance continue

La transformation de la menace a conduit à modifier l'organisation interne de l'ANSSI.

La principale évolution a consisté à détacher sa sous-direction du numérique (SDN) chargée jusqu'au 1er juillet 2020 de proposer, concevoir et mettre en œuvre des produits et des systèmes d'information sécurisés au profit des ministères, des opérateurs d'importance vitale et de l'ANSSI pour l'intégrer, avec le centre de transmissions gouvernemental (CTG) chargé de protéger les communications gouvernementales, dans l'opérateur des systèmes d'information interministériels classifiés (OSIIC), érigé en service à compétence nationale rattaché au SGDSN[121].

D'autres réorganisations, internes cette fois, sont intervenues. Elles sont, pour l'essentiel, récentes et correspondent à la mise en place de relais extérieurs à son action pour faire face à la diffusion de la menace : en particulier, la sous-direction des opérations (SDO) de l'ANSSI, qui porte le rôle de CERT-FR, a modifié sa composition interne et créé une nouvelle division écosystèmes, services et coopération (DESC). Chacun de ses bureaux permet de répondre à un type de solliciteur : bénéficiaires, partenaires, et relais du CERT-FR.

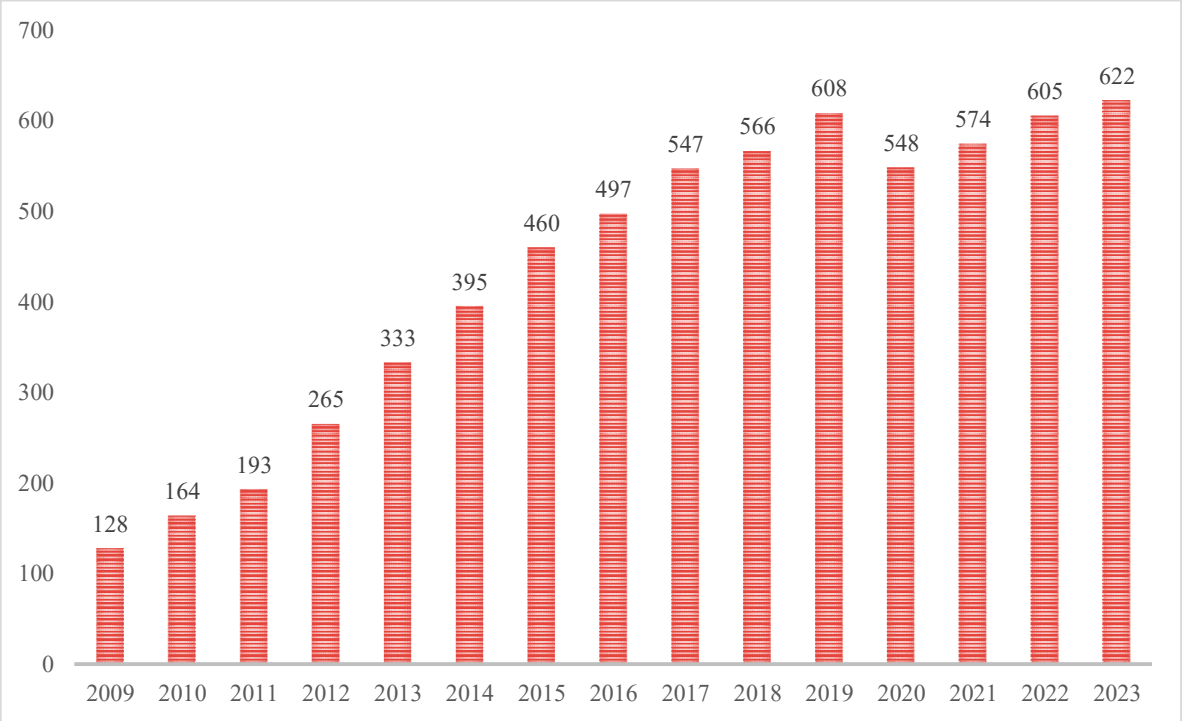
Ces évolutions ont été accompagnées par une forte progression des effectifs. L'agence est passée de 128 agents en 2009, date de sa création, à 622 agents en 2023 (contre 626 initialement prévus).

La rupture en 2020 s'explique par le transfert de la sous-direction du numérique de l'ANSSI vers l'OSIIC de 100 ETP. La création du nouvel opérateur Viginum a également amené une révision exceptionnelle du schéma d'emploi 2021, avec un prélèvement de 12 ETP. Le schéma d'emploi de l'ANSSI a ainsi été révisé à +28 ETP contre +40 par an, prévu initialement.

[120] 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.

[121] Décret n° 2020-455 du 21 avril 2020 portant création d'un service à compétence nationale dénommé « opérateur des systèmes d'information interministériels classifiés ». Il a la charge d'assurer les communications protégées des plus hautes autorités de l'État et développer les systèmes d'information interministériels classifiés.

Graphique n° 2 : Nombre d'ETP de l'ANSSI



Source : Cour des comptes d'après QP SE Affaires étrangères 18 PLF 2024 et questionnaire 1 ANSSI pour 2023 et réponse au ROP

Début 2024, le schéma d'emploi de l'ANSSI portait l'effectif civil de l'agence à 786 en 2027 mais la loi de finances 2025 a suspendu cette croissance continue et la trajectoire triennale du schéma d'emploi en stabilisant les effectifs 2025.

L'augmentation annoncée des moyens du BSI en Allemagne

L'agence allemande, le BSI (*Bundesamt für Sicherheit in der Informationstechnik*), rassemble environ 1 000 agents en 2021. La loi sur la sécurité numérique de 2021 prévoyait d'augmenter cet effectif de 800 agents à un rythme de 200 agents supplémentaires par an pendant quatre ans.

Cet accroissement doit répondre au souhait d'extension du périmètre d'intervention du BSI en matière de certification (Internet des objets, 5G), la protection des consommateurs, la cyberdéfense (détection, réponse à incident). Les ressources budgétaires ne sont pas connues. Elles ont toutefois bénéficié d'une enveloppe budgétaire exceptionnelle, comparable au dispositif France Relance, de 145 M€ sur trois ans. Ces crédits seront essentiellement investis dans la 5G.

La croissance des effectifs a entraîné une croissance de la masse salariale, notamment au cours des derniers exercices.

Tableau n° 10 : Masse salariale 2022 – 2024 en M€

	2022	2023 (prévisions)	2024 (prévisions)
Masse salariale (T2)	44,6	48,5	51,1

Source : ANSSI

Les crédits de fonctionnement sont également en progression.

Tableau n° 11 : Évolution du budget de fonctionnement 2020-2023 en M€

	2020	2021	2022	2023
Total AE initial	20,04	22,00	20,70	29,47
Total AE exécuté	18,81	19,68	22,38	32,69
Total CP initial	21,86	21,00	18,70	25,24
Total CP exécuté	21,54	18,92	20,52	22,50

Source : ANSSI

L'importance de la masse salariale dans les dépenses de fonctionnement de l'ANSSI s'explique par sa nature de centre d'expertise. Par ailleurs, ces crédits affectés à l'ANSSI ne tiennent pas compte des dépenses de fonctionnement non spécifiques comme celles relatives à l'immobilier, gérés par le SGDSN[122], par exemple, ni des dépenses d'investissement.

La Cour a relevé, dans un contrôle organique de l'ANSSI[123], que la croissance de l'entité a été réalisée sans projet de service. Ainsi, l'augmentation de 40 ETP par an qui a longtemps prévalu ne reposait sur aucun chiffrage concerté des besoins. À l'occasion de ses dix ans, l'ANSSI a organisé des « travaux stratégiques et collaboratifs : ANSSI10+ ». À l'issue, elle a produit un « manifeste », décliné en neuf commandements[124], comme autant d'orientations à mettre en œuvre. Mais ce document ne contient aucune perspective chiffrée des moyens nécessaires.

Elle a publié en mars 2025 un plan stratégique intitulé « Au cœur d'un collectif, pour une Nation cyber-résiliente ». Ce plan s'articule selon quatre axes : amplifier et coordonner la réponse cyber face à la massification de la menace, développer les expertises indispensables pour contrer les menaces cyber, promouvoir une action cyber européenne et internationale efficace, renforcer la prise en compte des enjeux sociétaux dans l'action de l'ANSSI. Ces axes sont déclinés en 11 objectifs. Parmi ceux-ci, l'élaboration d'un plan de transition vers la cryptographie post-quantique, et les travaux sur l'intelligence artificielle qu'elle s'assigne sont les principales nouveautés de son action. Ce plan, comme le manifeste précédent, ne formule qu'en termes généraux les activités de l'agence – se contentant par exemple, de vouloir mettre « *en œuvre une organisation adaptée pour s'assurer de prises de décisions impartiales dans les missions de contrôle* ». Il est surtout dépourvu de tout chiffrage, échéancier et définition des étapes nécessaires à la réalisation de ces objectifs. Les contraintes budgétaires, conjuguées aux évolutions nécessaires des missions de l'ANSSI (cf. *supra*), rendent pourtant nécessaire l'établissement d'un plan d'action précis, réaliste et assortis des ressources afférentes.

---

[122] Les crédits immobiliers gérés par le SGDSN atteignent 12,27 M€ en AE et 22,11 M€ en CP de fonctionnement courant immobilier dans le rapport annuel de performance – RAP - 2023.

[123] Observation définitives 2022 « DR-SF » sur le contrôle des comptes et de la gestion de l'ANSSI.

[124] « *Nous devons d'abord jouer à plein notre rôle d'éclaireur des transformations numériques. Nous devons sans cesse renforcer notre efficacité opérationnelle face à des menaces profondément changeantes, notamment face à la recrudescence des menaces de masse. Nous devons davantage mettre cette compétence au service de la formation en cybersécurité. Nous devons continuer à développer les synergies opérationnelles avec nos partenaires institutionnels nationaux. Nous devons accompagner la structuration de l'écosystème de cybersécurité. Nous devons renforcer notre engagement européen. Nous devons encore plus être une « administration orientée bénéficiaire ». Nous devons également renforcer notre culture interne de l'expérimentation et amplifier notre capacité d'innovation. Nous devons enfin renforcer l'accompagnement de nos agents.* »

Recommandation n°6. (SGDSN, ANSSI) Définir une programmation pluriannuelle des moyens de l'ANSSI cohérente avec la nouvelle stratégie nationale de cybersécurité et le plan stratégique 2025 de l'Agence.

CONCLUSION INTERMÉDIAIRE

Pour faire face aux cybermenaces, le SGDSN a été doté dès 2009 d'un service à compétence nationale dédié, l'ANSSI. Depuis, l'agence a développé une expertise reconnue au niveau national comme à l'international. Elle a déployé une gamme complète d'activités, au profit essentiellement des entités régulées. L'élargissement du périmètre de régulation, rendu nécessaire avec la nouvelle directive européenne NIS 2, doit la conduire à réviser ses moyens d'actions, et à s'appuyer sur des organismes relais, notamment pour l'assistance aux entités régulées et la qualification des solutions et produits de cybersécurité. En matière de réponse aux agressions, cette démarche doit être menée parallèlement à une articulation plus claire entre et avec les centres de réponse à incidents ministériels, sectoriels et territoriaux, et à la définition de leur financement pérenne.

L'ANSSI a bénéficié de moyens importants et croissants depuis sa création. La définition d'une nouvelle stratégie nationale de cybersécurité en 2024 conforte le pilotage centralisé du dispositif de lutte contre les cybermenaces. Elle l'oblige désormais à définir un véritable plan d'actions, décliné du plan stratégique 2025-2027 publié en mars 2025, et reposant sur un échéancier précis et une programmation des moyens nécessaires pour mettre en œuvre, notamment, le développement de ses fonctions renforcées d'observation et de contrôle.

4 UNE CYBERSECURITE A INTEGRER DANS LE FONCTIONNEMENT COURANT DES ENTITES REGULEES

L'action de l'État en matière de cybersécurité s'est traduite, outre sa réponse aux agressions, par le renforcement de la sécurité numérique de ses propres services mais également par la promotion d'un écosystème permettant l'émergence d'une offre de solutions et l'accompagnement des entités les plus fragiles. La formation des ressources humaines nécessaires à la sécurisation des systèmes d'information reste, par ailleurs, un enjeu majeur.

4.1 Dans le secteur public, mettre en place une politique ambitieuse de sécurité numérique, assortie d'une programmation pluriannuelle des ressources

Le panorama de la menace établi par l'agence européenne pour la cybersécurité (ENISA) en 2023 montre que les administrations publiques sont les secteurs les plus ciblés par les cyberattaques. La démarche de sécurisation des administrations publiques françaises a été déployée depuis 2014, selon des principes d'organisation inspirés de ceux applicables aux opérateurs d'importance vitales et aux opérateurs de services essentiels, mais sa concrétisation aura été tardive et financée essentiellement sur des crédits exceptionnels.

4.1.1 Une politique de sécurité des systèmes d'information mise en place très progressivement

La politique de sécurité des systèmes d'information de l'État (PSSI-E) a été fixée par la circulaire du Premier ministre n°5725/SG du 17 juillet 2014, élaborée par l'ANSSI en liaison avec les ministères. Elle est applicable également aux établissements publics sous tutelle d'un ministère, aux services déconcentrés de l'État et aux autorités administratives indépendantes. Elle édicte dix principes stratégiques et les traduit en objectifs et règles d'action qui concernent aussi bien la gouvernance, les ressources humaines, la gestion des biens, la gestion des risques, le traitement des incidents, la continuité de l'activité, les contrôles, que les différentes dimensions de la sécurité : physique, des réseaux, des systèmes d'information, du poste de travail, du développement des systèmes.

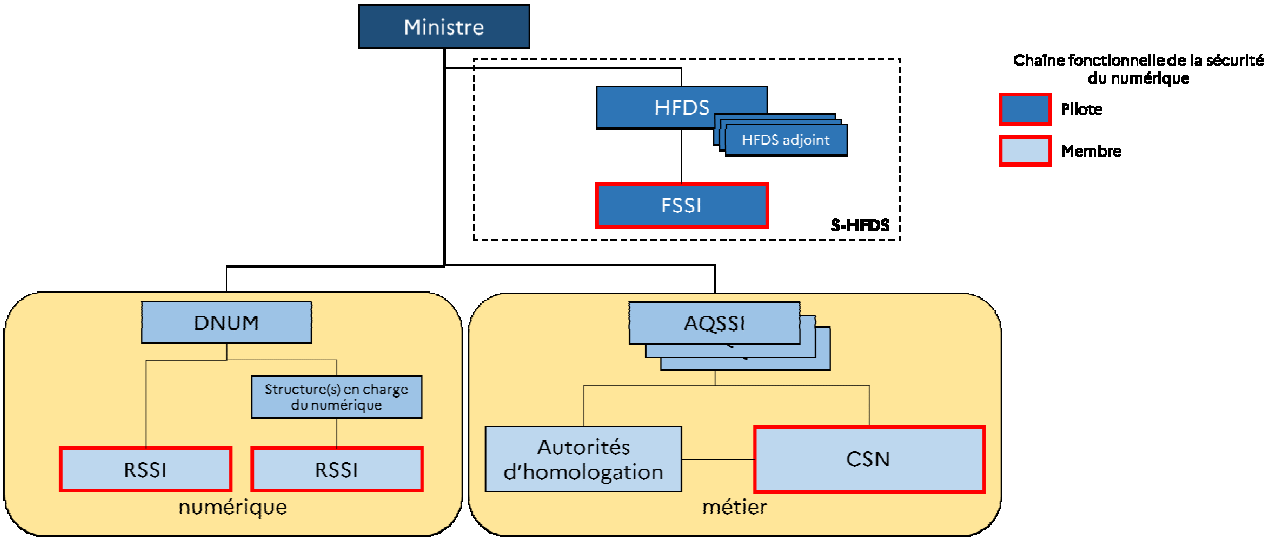
Récemment, la gouvernance de la sécurité numérique dans les services de l'État a été révisée par l'instruction générale interministérielle (IGI) n°1337 de 2021 (cf. *supra*). Ce texte assure, notamment, la mise en cohérence avec les principaux autres textes réglementaires[125] sur ce point.

[125] Notamment l'IGI 1300 sur la protection du secret de la défense nationale (nouvelle version approuvée par arrêté du 9 août 2021), décret n° 2019-1088 définissant le système d'information et de communication de l'État, les missions de la direction interministérielle du numérique, ainsi que le champ d'action des directions ministérielles du numérique.

Chaque ministère doit définir et mettre en œuvre une organisation en matière de sécurité numérique ; désigner et communiquer à l'ANSSI des coordonnées d'un point de contact sur les sujets relatifs à la sécurité numérique ; réaliser une évaluation annuelle du niveau de sécurité ; notifier les incidents de sécurité rencontrés.

Un modèle d'organisation est proposé (voir schéma ci-dessous).

Schéma n° 1 : Structuration ministérielle cible



Source : ANSSI

Si les adaptations sont possibles, la sécurité des systèmes d'information (SSI) repose dans chaque ministère sur un triptyque :

- le pilotage et le contrôle de la mise en œuvre de la politique ministérielle de sécurité numérique sont assurés par le fonctionnaire de sécurité des systèmes d'information, nommé par le ministre et placé sous l'autorité hiérarchique du haut fonctionnaire de défense et de sécurité ; il assure, en particulier, le secrétariat de l'instance stratégique ministérielle de la sécurité numérique et de l'instance ministérielle de pilotage de la sécurité numérique ;
- l'homologation de sécurité des infrastructures et services logiciels informatiques – c'est-à-dire l'attestation formelle précisant, dans le cadre du processus de sécurisation d'un système d'information, que les risques résiduels sont connus et maîtrisés - relève de la responsabilité des autorités qualifiées en sécurité des systèmes d'information (AQSSI) que sont les dirigeants des métiers dont les systèmes d'information sont supports (directeurs d'administration centrale, de services déconcentrés, des établissements publics, etc.), aidés par des conseillers à la sécurité numérique (CSN) ;
- l'expertise est portée, quant à elle, par le responsable de la sécurité des systèmes d'information (RSSI) au sein de la direction ministérielle du numérique (DNum), qui intervient au soutien des conseillers à la sécurité numérique (CSN).

À ce jour, les ministères ont adapté leur gouvernance en matière de sécurité numérique et ont désigné les conseillers à la sécurité numérique. En revanche, selon l'ANSSI, l'animation

des établissements publics nationaux en matière de sécurité numérique se met en place plus progressivement et diversement selon les contextes.

Si la gouvernance de la sécurité des systèmes d'information dans les ministères a été revue, les règles de sécurité applicables restent celles définies par la circulaire de 2014 et datent un peu. Leur révision est prévue mais, pour ne pas ajouter de la complexité au cadre de sécurité, un choix pertinent a été fait de procéder concomitamment à la refonte de la politique de sécurité des systèmes d'information de l'État et à la finalisation de la transposition de la directive NIS 2.

Parmi ces règles, figure, comme pour les OIV et les OSE, une obligation d'homologation de sécurité des infrastructures et services logiciels informatiques. La méthode suivie doit être adaptée aux enjeux du système d'information concerné et le niveau de sécurisation attendu dépend de l'intensité du risque et de la comparaison entre les coûts estimés de remédiation et le coût de la sécurisation. Actuellement, l'ANSSI travaille, dans ce sens, à la révision du guide relatif à l'homologation. Par ailleurs, elle a lancé et poursuit le développement de *Mon Service Sécurisé*, un téléservice qui guide et facilite l'homologation des services numériques classiques peu critiques des entités publiques.

Il convient de souligner, par ailleurs, que ni l'obligation de réaliser les audits subséquents à l'homologation et à son renouvellement ni un régime de sanctions des dirigeants, comparables à ceux définis pour les OIV / OSE, ne figurait dans la circulaire de 2014[126]. Si l'IGI n°1337 établit clairement la responsabilité des autorités qualifiées en sécurité des systèmes d'information (AQSSI), elle ne met en place aucun de ces leviers pour engager leur responsabilité et garantir ainsi un niveau satisfaisant de sécurité des systèmes d'information.

Les observations définitives de la Cour sur le plan de transformation numérique du ministère de la justice pointaient, par ailleurs, en janvier 2022, des défaillances importantes dans la démarche de sécurité numérique du ministère liées à un manque de ressources humaines, avec des conséquences importantes en matière d'homologation[127]. Depuis, le déploiement des homologations s'est poursuivi mais, fin 2024, 30 % seulement des systèmes d'information d'importance vitale ont été homologués (25/86), et les efforts en cours ne devraient permettre de couvrir que 46 % de ceux-ci, à un horizon encore indéterminé. Ces chiffres donnent la mesure à la fois de l'importance des travaux engagés et de la hauteur de la marche à franchir, au regard des ressources mobilisables. Ce sujet existe également dans les deux autres ministères relevant du périmètre de la présente enquête. Ainsi, le ministère de l'intérieur précise, en janvier 2025, qu'au total 101 systèmes d'information d'importance vitale, essentiels ou classiques ont été homologués en 2023-2024, dont les 28 systèmes d'information désignés comme essentiels pour les Jeux olympiques et paralympiques de Paris 2024.

La question de la responsabilité en matière de sécurité numérique dans les ministères doit être posée dans sa globalité, en tenant compte des ressources effectivement mises à disposition des AQSSI pour réaliser l'homologation des systèmes d'information dont ils ont la charge. La fixation d'objectifs précis de sécurisation de leur outils numériques apporterait une garantie sur ce sujet.

[126] Les systèmes d'information ministériels classifiés relèvent, quant à eux, de l'IGI n°1300.

[127] Cour des Comptes - Améliorer le fonctionnement de la justice – point d'étape du plan de transformation numérique du ministère de la justice - Communication à la commission des finances du Sénat - janvier 2022.

Recommandation n°7. (SGDSN) Renforcer la sensibilisation des dirigeants des services de l'État aux enjeux des cybermenaces et leur fixer des objectifs précis en la matière dans leur lettre de mission.

4.1.2 Le déploiement récent d'outils de détection et de prévention supplémentaires dans les services de l'État

La mise en place d'instruments automatisés de détection et de prévention dans les systèmes d'information des opérateurs régulés et de l'État permet de démultiplier les capacités de supervision de l'ANSSI. Cette dernière s'est servie des crédits qui lui ont été attribués dans le cadre du plan de relance 2020 pour financer les outils les plus récents.

Si les premiers outils ont été déployés à partir de 2013, l'ANSSI a engagé en 2019 un chantier majeur, en implantant des solutions de détection au cœur des systèmes ministériels, en commençant en priorité par les ministères régaliens. Sept ministères sont déjà intégrés au service de supervision sur une portion de leur système d'information.

L'ANSSI a aussi financé l'acquisition d'outils permettant des analyses approfondies sur les machines qui en sont équipées, et le blocage automatique des activités malveillantes. Dans ce cadre, l'ANSSI collecte et exploite les données produites mais les services ministériels disposent également de leur propre console de supervision, tout en bénéficiant du support et du maintien en condition opérationnelle de la solution.

L'ANSSI a également mis en œuvre en 2022 un dispositif de cyberdéfense automatisée permettant de bloquer certaines catégories d'attaques à large échelle, au niveau du service de résolution de noms[128], sur le réseau interministériel de l'État. Ce nouveau service de blocage est entré en production en septembre 2022. Depuis le 27 février 2023, il a permis de bloquer 60 attaques. 92 000 marqueurs différents ont été placés en blocage durant l'année 2023 et chaque mois, environ un milliard de requêtes sont traitées. Au total, le coût assumé par l'ANSSI pour cette prestation s'est élevé à 1,3 M€.

Le déploiement de ces outils confère à l'ANSSI une capacité de détection importante dans le périmètre des entités régulées. Ses restitutions aux entités supervisées sur le niveau de sécurité de leur annuaire gestionnaire des permissions d'accès[129] (service ADS), et sur leur niveau d'exposition sur Internet (service Silène) sont assorties de préconisations pour atteindre un niveau de sécurité à l'état de l'art.

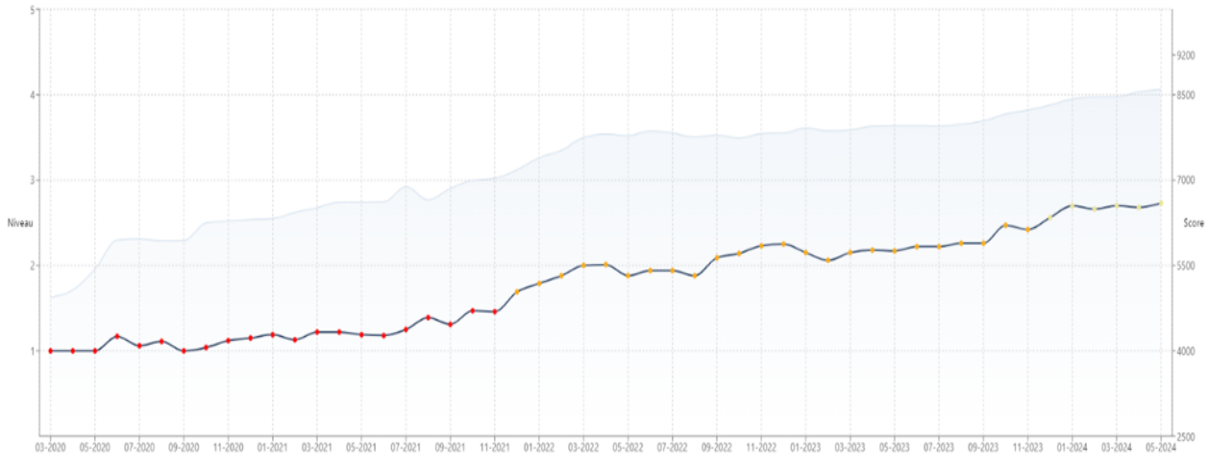
L'évolution des niveaux et des scores ADS est très satisfaisante dans les ministères[130].

[128] DNS : *Domain Name Service*

[129] L'annuaire Active Directory (AD) est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI. Le service ADS (Active Directory Security) est développé par l'ANSSI.

[130] L'exercice est encore à documenter pour l'exposition sur Internet.

Graphique n° 3 : Évolution des niveaux et scores ADS



Source : ANSSI

Ce renforcement notable de la sécurité numérique des ministères a été permis essentiellement par les financements exceptionnels de France Relance, et sous la pression de l'échéance des Jeux olympiques et paralympiques (JOP) de Paris 2024, comme cela a été également le cas pour la mise en place des centres de réponses à incidents.

4.1.3 Une évaluation de la maturité de la sécurité des systèmes d'information ministériels relancée récemment

La circulaire de 2014 emportait déjà l'établissement, par chaque ministère, d'un bilan annuel mesurant sa maturité globale en matière de sécurité de ses systèmes d'information. L'ANSSI a défini, de longue date, des indicateurs de performance sur la sécurité numérique des services de l'État, inscrits dans la présentation du budget de l'État. Mais ces indicateurs, peu précis, ne sont pas corrélés avec la gestion budgétaire des ministères. Dans le cadre de la nouvelle gouvernance de ce volet de la lutte contre les cybermenaces, il a été décidé en réunion interministérielle, outre le plan d'action cité *supra*, de lancer une campagne d'évaluation du niveau de maturité en cybersécurité de l'administration.

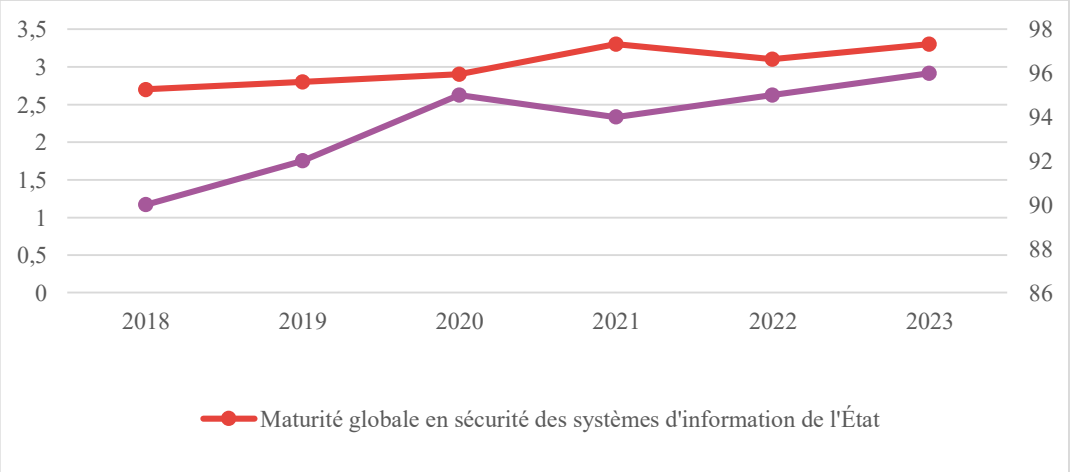
4.1.3.1 Des indicateurs de performance déconnectés des moyens mis à disposition dans le budget de l'État

Le projet annuel de performance du programme 129 « *coordination du travail gouvernemental* » comporte l'objectif d'« *améliorer la sécurité et la performance des systèmes d'information de l'État* ». Le suivi de la performance de l'État en la matière est réalisé au moyen

de l'indicateur 5.1 : « *Niveau de sécurité des systèmes d'information de l'Éta*t », décliné en trois volets dont deux relèvent de l'ANSSI[131] :

- la « *maturité globale en sécurité des systèmes d'information de l'État* » se présente sous la forme d'une note de 0 à 5, où 5 est l'optimum (axe gauche) et reflète l'écart entre un niveau de maturité effectif et un niveau de maturité considéré comme adéquat pour le ministère, en fonction de la sensibilité de ses systèmes d'information. Les niveaux atteints sont déterminés sur une base déclarative des ministères, encadrée par un guide méthodologique et un questionnaire, établis par l'ANSSI, en collaboration avec les départements ministériels[132] ;
- le « *niveau d'avancement des grands projets interministériels en matière de sécurité des systèmes d'information* » est établi par l'ANSSI qui le calcule en moyennant différentes données[133].

Graphique n° 4 : Sous-indicateurs de sécurité des systèmes d'information de l'État



Source : RAP du P129 Données fournies par l'ANSSI

Une amélioration de ces deux indicateurs est constatée sur les cinq dernières années, même si des à-coups sont perceptibles. Elle est liée, pour partie, au déploiement progressif d'outils de supervision par l'ANSSI.

[131] Un troisième indicateur de la sécurité des systèmes d'information n'a été introduit qu'en 2022 et vise les systèmes d'information interministériels classifiés - ISIS, OSIRIS et HORUS - qui relèvent désormais de l'OSIIC. Un autre indicateur 5.2 Taux de sites sensibles ayant subi un incident dont la durée globale est supérieure à 4 h est restreint au réseau interministériel de l'État (RIE) - réseau informatique étendu raccordant les services de l'État français sur l'ensemble du territoire national- et suivi par la DINUM (cf. rapport 2024 de la Cour des comptes sur la DINUM).

[132] Les données fournies par les ministères peuvent éventuellement être corrigées à partir des constats faits par l'ANSSI, lors de ses inspections.

[133] Le taux de connexion des passerelles des organismes de l'État au centre gouvernemental de détection des attaques informatiques ; le taux de déploiement des systèmes d'information sécurisés par rapport à une cible (notamment le réseau téléphonique sécurisé OSIRIS, et l'intranet gouvernemental ISIS) ; le pourcentage de produits labellisés par l'ANSSI par rapport à des objectifs pour chaque catégorie de produits. De nouvelles catégories peuvent être ajoutées chaque année, pour suivre l'évolution des technologies et de la menace.

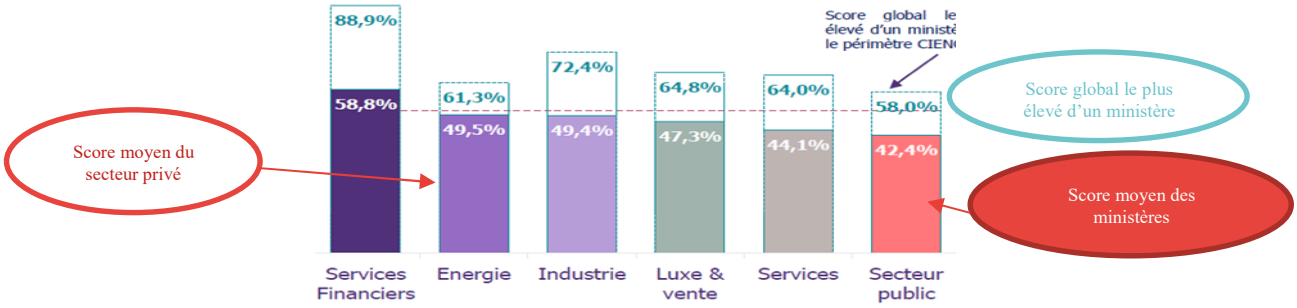
La présentation des crédits destinés à la politique de sécurité des systèmes d'information ne traite que du pilotage assuré par le SGDSN, au travers de l'ANSSI, et ne tient pas compte des dépenses réalisées dans les ministères en matière de sécurité numérique. De fait, ces dépenses ne sont pas identifiées dans les comptes des ministères où elles se confondent avec les dépenses numériques. La levée progressive de leur « *dette technologique* », au travers de plans de transformation numérique, devrait permettre une amélioration substantielle de la sécurité des systèmes d'information, grâce à sa prise en compte dès l'expression du besoin opérationnel et la conception des équipements (sécurité dite *by design* ou embarquée, recommandée par l'ANSSI). Cependant, la sécurité des systèmes d'information doit être pensée aussi bien au moment de l'achat des systèmes d'information que dans le cadre de leur maintenance ou d'une adaptation aux cybermenaces.

4.1.3.2 Une évaluation approfondie de la maturité de la cybersécurité dans l'administration de l'État toute récente

Une étude visant à apprécier la maturité en cybersécurité des directions centrales des ministères, financée elle aussi par le plan France Relance de 2020, a été récemment conduite et confiée à un prestataire de service. Après une phase pilote réalisée de septembre 2021 à juin 2022 sur trois ministères - ministères chargés des affaires étrangères, de l'intérieur et de l'économie -, pour éprouver la méthodologie, la généralisation du dispositif a été validée par les HFDS lors du comité stratégique interministériel de la sécurité numérique de mars 2022. Les derniers comptes rendus ont été établis à l'automne 2023.

L'enquête a porté sur différentes directions d'administration centrale de 11 ministères, soit 80 entités[134]. Elle fonde ses analyses sur des référentiels internationaux (notamment le référentiel NIST[135]) et une comparaison avec plus de 70 grands groupes privés, évalués selon la même méthodologie.

Graphique n° 5 : Score de maturité par secteur d'activité



Source : Enquête sur la maturité de la cybersécurité dans les administrations centrales

[134] Les services déconcentrés ne faisaient pas partie du périmètre de l'évaluation.

[135] Le *National Institute of Standards and Technology* (NIST) est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des normes de concert avec l'industrie. Il a produit un référentiel de cybersécurité qui est l'un des cadres de sécurité les plus largement adoptés par l'ensemble des industries américaines.

L'évaluation globale confirme une maturité du secteur public perfectible. Alors que la cible usuelle de sécurité par rapport aux référentiels est fixée à 65 %, le score de maturité du secteur public inclus dans le champ de l'enquête est de 42,4 %. Par comparaison, le score global du secteur privé enquêté est de 49,4 %, avec des variations sensibles selon les secteurs d'activité.

Les variations entre ministères – voire entre directions au sein des ministères – sont également importantes, puisque le meilleur score s'établit à 58,0 %. Deux groupes se distinguent et celui des ministères régaliens dispose d'un niveau de protection sensiblement supérieur à celui des autres ministères.

Au-delà de l'évaluation globale, l'enquête identifie, pour chaque ministère, ses forces et ses faiblesses sur les différents axes de sécurité définis dans le référentiel NIST - identifier, détecter, protéger, répondre, reconstruire – et fournit des recommandations très précises et spécifiques pour améliorer leur performance de cybersécurité. Elles sont un élément à prendre en compte pour tracer une feuille de route spécifique à chacun d'entre eux.

L'IGI 1337 dispose qu'« *une convention entre l'ANSSI et chaque ministère précise les relations entre les parties et décrit les services auxquels recourent les ministères ainsi que les modalités et responsabilités associées* ». Ces conventions, qui à ce jour restent à élaborer, pourraient servir de support à un engagement ministériel sur des objectifs pluriannuels à atteindre en matière de cybersécurité, définissant un échéancier d'actions et les moyens à mettre en œuvre et traduit dans la programmation budgétaire. Pour la construire, il est possible de se référer aux constats établis dans le privé par l'enquête. Elle indique que, dans les grands groupes privés, la part du budget numérique consacré à la cybersécurité est de 5,5 % et le ratio moyen d'ETP cyber est d'un ETP pour 1 199 agents.

Recommandation n°8. (SGDSN, ANSSI) Conformément à l'IGI 1337, établir des conventions entre le SGDSN, l'ANSSI et chaque ministère, fixant les objectifs pluriannuels à atteindre en matière de cybersécurité, un échéancier d'actions et les moyens à mettre en œuvre.

4.2 La construction inachevée d'un écosystème de la cybersécurité

La protection de la société face aux cybermenaces est un des trois piliers de l'action de l'État en matière de cybersécurité civile. Le Livre blanc de 2008, déjà, assignait à la future ANSSI une participation *« à la diffusion de la sécurité dans la société de l'information* » et soulignait la nécessité d'établir « *une stratégie industrielle, permettant le renforcement de capacités nationales de conception et de réalisation dans le domaine de la sécurité des systèmes d'information* ». Cette mission, formalisée dans un document militaire et de défense, constitue la déclinaison, dans le domaine civil, de l'activité de la direction générale de l'armement, au cœur de la base industrielle et technologique de défense qui regroupe l'ensemble des entreprises de défense qui contribuent à concevoir et à produire les équipements pour les armées. Pour autant, les moyens affectés à l'industrie de défense et ceux mis à la disposition de la cybersécurité civile sont incommensurables et ces derniers apparaissent, somme toute, modestes. L'émergence de certains dispositifs a précédé la définition de leur modèle

économique et les mécanismes d'accompagnement des entités les plus fragiles vers la sécurité numérique ont été déployés de manière profuse, rendant le système difficilement lisible.

4.2.1 Les politiques industrielles de la cybersécurité : des crédits limités, essentiellement destinés au secteur public

Le développement de l'écosystème en cybersécurité a bénéficié de politiques volontaristes, inscrites dans des plans successifs de relance économique et de politique industrielle, alimentés pour certains d'entre eux par des crédits européens, depuis plus de 10 ans. En effet, dès 2013 avec le programme « Nouvelle France Industrielle », un volet cybersécurité a été inscrit dans les différents plans nationaux.

Le programme « Nouvelle France Industrielle »

Lancé en 2013, ce programme comportait 34 « plans industriels » dont un consacré à la cybersécurité. Il s'agissait déjà de développer une industrie performante de cybersécurité française, pour sécuriser les infrastructures vitales du pays, selon un principe de souveraineté, tout en favorisant une opportunité de créations d'emplois. L'industrie de la cybersécurité française représentait alors 40 000 emplois et un chiffre d'affaires de 13 Md€.

Le directeur général de l'ANSSI était chef de projet de ce plan. Ces travaux ont notamment abouti à :

- la création du label France Cybersécurité, attestant que les produits et services qui portent le label sont français et qu'ils possèdent des fonctionnalités claires et bien définies, avec un niveau de qualité vérifié par un jury indépendant qui se base sur des certifications existantes, une investigation par un tiers expert indépendant et des retours d'utilisateurs. Ce label est gouverné par une structure tripartite composée de représentants des utilisateurs, de représentants des industriels et des services de l'État compétents, qui en définit le cahier des charges et les principes de délivrance et de retrait (mise en place du jury d'attribution notamment) ;
- la création du fonds Brienne III, afin d'apporter des capitaux - de 10 à 50 millions d'euros - à des entreprises innovantes du secteur (start-ups et entreprises en croissance et à fort potentiel) développant des cybertechnologies de rupture pour les aider à concrétiser leurs plans de croissance[136] ;
- et à la sensibilisation de l'écosystème aux enjeux de confiance du numérique.

La Cour a examiné plus précisément les volets cyber des plans les plus récents, France Relance en 2020, France 2030 en 2022.

4.2.1.1 Un volet cyber du plan de relance essentiellement orienté vers la sécurisation des SI du secteur public

À la suite de la crise sanitaire, le plan France Relance a été adopté le 3 septembre 2020. Il a été doté de 100 milliards d'euros, et soutenu financièrement à hauteur d'environ 40 milliards d'euros par l'Union européenne, au titre de son propre plan de relance « Next Generation EU ». Ce plan d'investissements français comprenait trois priorités : la transition écologique

[136] Un partenariat entre la société gestionnaire du fonds et l'ANSSI permet aux investisseurs du fonds Brienne III de bénéficier de l'expertise de celle-ci, notamment dans le choix des sociétés cibles. Ce partenariat complète celui déjà en place, signé le 3 octobre 2019 entre la société gestionnaire et la ministre des armées, permettant au fonds d'accéder à son réseau d'experts (DGA, DGSE, COMCYBER et l'Agence Innovation de Défense).

(30 milliards d'euros) ; la compétitivité et l'innovation (34 milliards d'euros) ; la cohésion sociale et territoriale (36 milliards d'euros). 1,7 milliards d'euros ont été consacrés à la transformation numérique de l'État et des territoires.

Les montants affectés à la cybersécurité sont beaucoup plus modestes : 136 M€ sur la période 2021-2022, portés à 176,9 M€ début 2022 (soit environ 10,5 % des crédits de transformation numérique). Ils sont compris dans le volet « compétitivité et innovation », porté par le programme 363 « compétitivité », sous la responsabilité de la direction du budget, et gérés par le SGDSN, au titre d'une délégation de gestion[137].

Le volet cybersécurité a principalement permis de renforcer la sécurité numérique des entités publiques et l'effet sur l'offre a été indirect, du fait du fléchage des solutions de sécurisation attendues vers des éditeurs européens.

Les ministères ont bénéficié de 32 M€ (soit 18,1 % du volet cybersécurité) pour sécuriser des réseaux de l'État et déployer de nouveaux services mutualisés et produits au profit de leurs agents (cf. *supra* 4.1.2). L'essentiel a, pour autant, visé le secteur public territorial (établissements publics locaux, collectivités territoriales), au travers de trois autres chantiers :

- le soutien financier à des projets de cybersécurité pour les collectivités territoriales, en mettant à la disposition de leurs structures fédératrices (syndicats, groupements d'intérêt public, établissements publics), spécialisées dans l'accompagnement à la transformation numérique, un dispositif d'acquisition de produits et de licences mutualisés au profit de leurs membres (27,6 M€, soit 15,6 %) ;
- le soutien à la création d'un réseau de centres de réponse à incident (CSIRT) régionaux et sectoriels (cf. 3.1.3), notamment dans les secteurs critiques (dont le maritime, l'aérien et la santé) et auprès des acteurs essentiels du tissu socio-économique territorial (17,3 M€, soit 10,0 %) ;
- le financement de produits et prestations de cybersécurité au profit prioritairement des collectivités territoriales et des établissements de santé, dans le cadre des « Parcours de cybersécurité » (100 M€, soit 56,5 % des crédits de cybersécurité) (cf. annexe n°3).

Ces crédits sont relativement limités. Ils financent, de manière exceptionnelle, des solutions qu'il est nécessaire de pérenniser car elles contribuent au fonctionnement courant des entités concernées.

4.2.1.2 Un plan France 2030 qui accorde une place modeste à la cybersécurité

En 2022, le plan France 2030, en intégrant les crédits du Programme d'investissements d'avenir (PIA) 4, a permis d'afficher un total de 54 Md€ pour le soutien de la recherche et du tissu industriel. Le PIA 4 comportait 23 stratégies d'accélération, dont six liées au secteur du numérique : cloud (550 M€), intelligence artificielle (820 M€ portés à 871 M€ fin 2024),

[137] Il est ainsi devenu responsable du budget opérationnel de programme (BOP) « 363 SGDSN », chargé de financer les dispositifs visant le renforcement du niveau de sécurité du socle numérique de l'État via le déploiement d'une offre de services de cybersécurité ; l'accroissement de la couverture des systèmes de détection et de la réponse à incidents. Ce BOP est composé de 12 unités opérationnelles (UO), une UO regroupant les dépenses ordonnancées par le SGDSN lui-même (UO « SGDSN – ANSSI ») et 11 UO ministérielles pour lesquelles des conventions de délégations de gestion ont été signées avec les ministères concernés).

technologiques quantiques (510 M€), 5G et futures technologies de communications (530 M€), verdissement du numérique (50 M€), cybersécurité, pour un montant passant de 376 M€ à 322 M€. La cybersécurité ne représentait ainsi que 11,4 % crédits en faveur du numérique. Les montants consacrés à la sécurité numérique restent donc, somme toute, relativement modestes, même si des dépenses en faveur d'innovations numériques peuvent également répondre directement ou indirectement aux enjeux de cybersécurité.

Il est intéressant de noter que les actions menées en faveur de la cybersécurité ne participent pas des dix objectifs identifiés dans le plan mais des conditions jugées indispensables à leur réalisation, parmi lesquelles[138] figure le développement de « *solutions nationales en matière de logiciels, dans les domaines de l'intelligence artificielle, de la cybersécurité, du cloud et du calcul quantique* ». La cybersécurité apparaît ainsi positionnée, assez pertinemment, non comme une fin en soi mais comme un élément de fonctionnement courant des entités économiques, avec un enjeu de souveraineté numérique.

Par ailleurs, si les objectifs affichés par la stratégie d'accélération de la cybersécurité visent essentiellement les entreprises privées, fin 2023, elles représentaient seulement 37 % des aides attribuées[139], soit 65,7 M€ pour les petites et moyennes entreprises (PME), 9,5 M€ pour de grandes entreprises et 6,3 M€ pour les entreprises de taille intermédiaire (en subventions et avances, pour un total de 81,5 M€). L'essentiel des financements a été orienté vers les établissements publics de recherche et de formation, et notamment l'institut national de recherche en informatique et en automatique (INRIA) qui a bénéficié de 56,1 M€ au titre du programme et équipements prioritaires de recherche (PEPR) cybersécurité à hauteur de 16,1 M€ et du programme de transfert des compétences (*i.e.* le passage de la recherche à l'industrie), pour près de 40 M€.

Enfin, le plan France 2030 poursuit les réalisations du plan de relance en direction des collectivités territoriales, au travers d'une délégation de crédits du SGPI à l'ANSSI d'un montant limité (1 M€ en AE / CP sur la durée du projet), pour accompagner de nouvelles collectivités territoriales dans de nouveaux parcours de cybersécurité. Ils recouvrent également, à hauteur de 2,5 M€, la contribution de l'État à la création d'une plateforme sécurisée dédiée aux collectivités territoriales, comprenant notamment un nom de domaine, un serveur mail et un espace de stockage minimal sécurisé. La convention signée à cette fin, le 7 décembre 2023, entre le SGDSN / ANSSI et l'agence nationale de la cohésion des territoires (ANCT) concrétise une des ambitions inabouties du plan de relance : promouvoir des outils et services mutualisés dans le but d'améliorer au moindre coût la sécurité numérique, notamment des communes rurales et / ou de taille modeste.

[138] Les autres conditions sont : « *Sécuriser, autant que possible, l'accès aux matériaux (métaux, plastiques, bois, …) ainsi qu'aux composants stratégiques, notamment électronique, robotique et machines intelligentes ; développer les talents en construisant les formations de demain ; investir y compris en capital pour aider nos innovations à émerger et s'industrialiser et aider nos start-ups à accélérer leur croissance* ». Ces conditions guident également l'action en faveur du développement de la sécurité numérique.

[139] Les établissements publics, principalement de recherche et de formation, ayant bénéficié de 61 % des crédits engagés, qui s'élevaient à 221,8 M€ fin 2023.

4.2.2 La création d'outils de cybersécurité dont les missions et le modèle économique sont affinés *ex-post*

La réaction aux cybermenaces a conduit à mettre en place des outils avant même de définir précisément leurs missions ou leurs modalités de financement.

4.2.2.1 La plateforme Cybermalveillance, un outil numérique *sui generis*

Le groupement d'intérêt public (GIP) ACYMA, regroupant 64 acteurs publics et privés, « incubé » par l'ANSSI en 2016-2017, est destiné à sensibiliser les particuliers, entreprises et collectivités territoriales aux cybermenaces. Il gère, depuis son ouverture en octobre 2017, la plateforme *Cybermalveillance.gouv.fr*. Cette plateforme informatisée met à disposition divers contenus thématiques dans la prévention et la sensibilisation aux dangers du numérique – dont un kit de sensibilisation qui regroupe différents supports (fiches, mémos, vidéos) sur des bonnes pratiques de cybersécurité et des recommandations pour réagir face aux actes de cybermalveillance les plus courants - et un système d'alerte de sécurité sur l'actualité des risques majeurs.

Elle propose également un parcours d'assistance aux victimes d'actes de cybermalveillance qui comprend trois temps : l'établissement d'un diagnostic de la situation ; des conseils pratiques pour comprendre l'incident et entreprendre les actions pour le résoudre, dont le dépôt de plainte auprès des services de police ou de la gendarmerie ; la mise en relation avec des professionnels spécialisés en cybersécurité experts susceptibles d'apporter une assistance technique, labellisés Expert-cyber par le GIP.

Le GIP Acyma développe ses prestations à partir d'une équipe et d'un budget relativement modestes.

Tableau n° 12 : Recettes (en €) et ETP du Gip Acyma

	2020	2021	2022	2023
Recettes	1 399 500	2 210 500 €	1 961 000	3 066 950
ETP	12	13	17	19

Source : GIP Acyma

La structure est portée par les contributions des membres des différents collèges, et notamment une subvention du SGDSN / ANSSI (845 000 € en 2023). Celle-ci n'avait pas vocation pourtant à être pérenne et le GIP devait définir son modèle économique et trouver des financements réguliers issus de son activité. Ce point n'est pas tenu alors que la plateforme a une utilité reconnue.

Pour autant, le GIP a étendu ses missions et obtenu le soutien – y compris financier – du ministère de l'intérieur, pour développer, à partir de 2022, pour réaliser un équivalent numérique de « l'appel 17 » afin que « *chaque citoyen puisse signaler en direct une attaque cyber et être mis immédiatement en relation avec un opérateur spécialisé* ». Les victimes peuvent accéder, via la plateforme, à un opérateur de la police ou de la gendarmerie pour les guider dans le dépôt de leur plainte. Le GIP a travaillé avec le ministère de l'intérieur sur la

conception d'outils d'aides à la décision pour les opérateurs de la police et de la gendarmerie, afin de les accompagner dans leurs échanges avec les victimes. Ce service a fait l'objet d'une subvention exceptionnelle de 700 000 € en 2023 et le « 17 Cyber » est opérationnel depuis le 17 décembre 2024.

En revanche, alors que le GIP Acyma avait été associé au projet de filtre national de cybersécurité anti-arnaque, sa participation a été finalement récusée. L'obligation légale faite aux acteurs économiques assujettis (fournisseurs d'accès à internet, fournisseurs de navigateurs web, fournisseurs de service de résolution de noms de domaine, moteurs de recherche, annuaires) de filtrer les contenus qui leur seront signalés par l'autorité publique reste en attente de ses décrets d'application et d'autres options sont à l'étude pour diffuser les alertes afférentes au grand public.

La question d'une définition claire des missions et d'un financement pérenne du GIP Acyma reste donc posée.

4.2.2.2 Le Campus Cyber : le développement d'un lieu « totem », insuffisamment mûri

À la demande du président de la République, le Premier ministre a mandaté le futur président directeur général du Campus Cyber, en juillet 2019, pour développer le projet, inspiré de Beer-Sheva en Israël, Skolkovo en Russie ou encore New York avec le Global Cyber Center. Les objectifs étaient de promouvoir l'expertise nationale et de rapprocher la recherche publique et les industriels pour faire émerger des licornes en cybersécurité. Il s'agissait donc de créer une synergie de l'écosystème de cybersécurité, en l'incarnant physiquement dans un lieu « totem ». Le projet, validé à l'automne 2020, a été inauguré le 15 février 2022, en présence du ministre de l'économie.

Lors de la création du Campus Cyber, l'agence des participations de l'État (APE), a investi au capital de la société par action simplifiée (SAS) à hauteur de 3,5 M€ (soit 40 % du capital total de 8,9 M€). Ce faisant, l'État est représenté par l'ANSSI au sein du conseil d'administration et de l'assemblée générale. D'autres ministères[140] sont également partie prenante au sein du collège « institutionnel » de la gouvernance de la SAS afin de veiller à la bonne articulation du Campus Cyber avec la puissance publique et Bpifrance dispose d'un siège d'observateur au sein du Conseil d'administration. 25 % des espaces sont réservés à l'État – l'ANSSI y occupe un étage complet[141] et y accueille son centre de formation, l'InterCERT et une partie du GIP Acyma.

L'objet social recouvre la gestion de locaux et d'équipements professionnels, mais également une mission de soutien à la mise en commun de ressources et de projets, en matière de cybersécurité. Il identifie de manière précise la gestion d'un « incubateur » et la promotion de campus cyber territoriaux. À ce jour, le Campus Cyber remplit son engagement en matière de gestion des locaux et d'évènements. Il constitue également une vitrine à l'international pour la cybersécurité française : après deux ans d'existence, il abrite ainsi 6300 résidents, 500

[140] Composition du collège Institutionnel : ANSSI, CNIL, GIP ACYMA, ministère de la justice, ministère de l'économie et des finances, ministère de l'intérieur, ministère des armées. Les ministères de l'éducation nationale et le ministère de l'enseignement supérieur et de la recherche sont membres du collège Formation.
[141] En plus des locaux parisiens de l'Hôtel des Invalides et de la tour Mercure et de son antenne à Rennes.

étudiants y suivent leur formation, plus de 100 délégations françaises, européennes et internationales y ont été reçues, plus de 750 évènements professionnels y ont été organisés.

S'il revendique 650 experts ayant contribué aux groupes de travail menés en commun et un certain nombre de publications produites dans ce cadre[142], l'animation du collectif reste complexe. Elle se heurte, en effet, à l'exigence du secret au sein de services présents de l'État (ANSSI mais également DGSI, et représentants du ministère des armées) et à la protection du secret commercial et de la propriété intellectuelle pour les entreprises privées. Sur ce dernier point, en particulier, la signature d'une charte rappelant les exigences afférentes – et notamment une clause de « non débauchage » - est obligatoire pour l'ensemble des membres. La mise en place de produits et de services communs – y compris en matière de formation – s'en trouve donc bridée.

À ce jour, au-delà de l'activité de gestion locative de ses espaces, le fonctionnement du Campus Cyber pour sa mission d'animation est assuré, pour quatre ans (jusqu'en août 2025), par une subvention de l'État versée via Bpifrance de 4,3 M€, soit la moitié du budget prévisionnel de cette activité.

Cette activité d'animation de l'écosystème cyber est renforcée par le portage de deux projets financés par France 2030 et d'autres collectivités publiques – européenne et territoriale.

Lauréat de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » émis dans le cadre de France 2030, le Campus Cyber assure le pilotage d'un consortium dénommé TAL-CYB qui réunit 13 partenaires qui visent à remédier au déficit de talents cyber en France. Sur une enveloppe globale de 18,6 M€ échelonnée sur cinq ans, 3,1 M€ sont fléchés vers les Campus Cyber, pour assurer la gouvernance et le suivi administratif et financier du dispositif et assurer la réalisation de quelques actions. Il s'agit principalement de gestion d'évènements (dont *escape game*, *serious games*) et du développement d'une plateforme de ressources et d'aide à l'orientation vers les formations et métiers cyber.

Un autre consortium a été créé dans le cadre du programme « Cybersécurité et Intelligence Artificielle Hub » (CYBIAH). L'objectif est de renforcer la résilience des PME, et des collectivités locales face aux menaces croissantes en cybersécurité, en fournissant un accompagnement complet incluant des diagnostics techniques, des formations et des solutions de sécurisation adaptées. D'ici à mai 2026, 150 PME et 30 collectivités de la région Île-de-France doivent en bénéficier. Le Campus Cyber se positionne comme tiers de confiance entre les PME et les offreurs cyber en facilitant la rencontre entre l'offre et la demande, soulignant par là même le défaut de lisibilité des dispositifs d'aide existants. Les financements du projet (5 M€) proviennent de plusieurs sources : Commission européenne dans le cadre de son programme DIGITAL Europe (3 M€ couvrant 50 % des activités) ; région Île-de-France (2 M€) ; métropole du Grand Paris (MGP) depuis mai 2024 (150 000 €).

La fonction d'animation de l'écosystème assurée par le Campus Cyber manque donc, pour le moment, d'une assise pérenne. Alors que des campus cyber se développent dans les territoires – les projets étant aboutis en Bretagne, Nouvelle Aquitaine et Hauts-de-France -, deux ans après sa création, les questions du modèle économique sous-jacent et du statut du Campus Cyber sont clairement posées.

[142] Le site internet du campus cyber permettait d'identifier, en mars 2024, 22 productions réalisées en commun, comme « post-quantum cryptography – sensibilisation » ou « l'intelligence artificielle en cybersécurité ».

À la suite du conseil d'administration du 12 juin 2024, une réflexion sur la vision, les missions et priorités du Campus Cyber pour les cinq prochaines années est prévue, en partenariat avec l'ANSSI. Elle devra embarquer la DGE et les représentants des régions, chargés de l'animation économique des territoires ainsi que les représentants des demandeurs visés (petites et moyennes collectivités et structures intercommunales, PME et TPE) et inclure une étude sur la pertinence du statut juridique de l'entité.

Recommandation n°9. (SGDSN) Proposer un modèle économique pérenne de fonctionnement pour le GIP Acyma et le Campus cyber.

4.2.3 L'accompagnement de l'écosystème, une réorientation récente vers les acteurs les plus fragiles

L'évolution de la menace, et notamment le ciblage des acteurs du « bout de chaîne », a conduit à déployer récemment un arsenal de mesures d'accompagnement dans leur direction. Cette démarche se caractérise par une profusion d'outils et d'intervenants qu'il conviendra de rationaliser, tant dans la labellisation des solutions de cybersécurité que dans l'accompagnement des acteurs locaux fragiles.

4.2.3.1 Une animation des territoires par les services de l'État à mieux coordonner

L'ANSSI a mis en place de longue date des coordinateurs sectoriels, rattachés à la sous-direction de la stratégie. Ces coordinateurs sectoriels sont les représentants du secteur au sein de l'agence et vis-à-vis de ses principaux acteurs (avec un rôle déjà mentionné *supra* en matière de programmation et de préparation des audits), et, réciproquement, les garants du bon déploiement des réglementations et bonnes pratiques de cybersécurité dans leur secteur.

S'ils étaient, dès l'origine, chargés d'analyser la structure et les besoins du secteur, les relations étaient principalement établies avec les administrations, les OIV et les OSE. Les plus récentes fiches de poste mettent l'accent sur la prise en compte de l'ensemble du secteur d'activité et la globalité de la chaîne de valeur. Il leur revient, à ce titre, de porter « *une vision stratégique fixant des ambitions en matière de cybersécurité pour le secteur* », et de la traduire en « *un plan d'action à mettre en place au sein de l'Agence* ».

Par ailleurs, à partir de décembre 2015, l'ANSSI a recruté des délégués territoriaux, également rattachés à la sous-direction de la stratégie. Ce dispositif compte aujourd'hui 17 personnes, dont 14 délégués territoriaux (un par région et un pour les territoires d'outre-mer). Leur mission est d'incarner l'agence – comme ambassadeurs et comme « capteurs » – en région, d'aider à la naissance et au développement des projets et initiatives cyber sur le territoire, de porter la politique industrielle de l'ANSSI, participer au développement des talents en sécurité des systèmes d'information, contribuer à la sécurité économique et à l'animation d'un écosystème cyber régional, conduire des actions de sensibilisation et de conseils, etc. Comme en ont témoigné des acteurs territoriaux, l'identification d'un délégué territorial facilite, effectivement, les relations avec l'ANSSI et permet une meilleure réactivité de l'ensemble.

Cependant, alors que des territoires sont particulièrement investis par certains secteurs d'activité, la liaison entre les deux compétences, délégués sectoriels et territoriaux, n'est pas expressément organisée mais se réalise dans l'appartenance à une même sous-direction.

Par ailleurs, l'action des délégués territoriaux nécessite d'être mieux articulée avec l'action préfectorale. Outre l'animation de la politique de sécurité numérique des services déconcentrés de l'État, les préfets de région et de département sont investis d'une politique de sensibilisation à la cybersécurité. La note du secrétaire général du ministère de l'intérieur, haut fonctionnaire de défense et de sécurité, du 20 avril 2022 les invite à définir un programme régional en se coordonnant avec le délégué régional de l'ANSSI. En revanche, la prévention et la gestion d'une attaque numérique à fort impact sur la vie économique et sociale relève de l'état-major départemental de sécurité dans sa dimension numérique, qui réunit autour du sous-préfet référent numérique, le conseiller à la sécurité numérique et les référents départementaux de police et de gendarmerie. Il conviendrait d'y associer les délégués de l'ANSSI.

Par ailleurs, les relations entre les délégués territoriaux de l'ANSSI et les délégués à l'information stratégique et à la sécurité économiques (DISSE)[143] de la DGE, en charge de la sécurité économique, relèvent pour le moment de l'*intuitu personae* et il serait intéressant qu'elles soient également coordonnées.

4.2.3.2 Des aides multiformes, des acteurs multiples

Comme le souligne la direction générale des entreprises, le niveau de sécurité d'une chaîne de valeur dépend de la sécurité du maillon le plus faible et la diffusion de la culture de la cybersécurité auprès des TPE et des PME peut relever de l'impératif de sécurité nationale pour certains secteurs. Les TPE, PME et ETI représentaient, en 2022, 40 % des attaques par rançongiciel traitées ou rapportées à l'ANSSI. Seul un tiers des TPE et PME est considéré comme correctement sécurisé. Pourtant, les conséquences d'une cyberattaque sont dramatiques : le risque de défaillance de l'entreprise augmente d'environ 50 % dans les 6 mois qui suivent l'annonce de l'incident, selon la récente étude d'un assureur.

Dans ce domaine de l'accompagnement, l'action est également profuse.

L'action des régions est importante, relayée souvent par les chambres de commerce et d'industrie. À titre d'exemple, la région Île-de-France aide les PME et les associations régies par la loi de 1901 au travers de deux dispositifs : chèque diagnostic Cyber qui vise à aider les PME à identifier les actions prioritaires à mettre en œuvre, avec une aide pouvant aller jusqu'à 5 000€ ; chèque investissement cyber pour renforcer leurs dispositifs de sécurité (jusqu'à 2 500 € pour les TPE et jusqu'à 10 000 € pour les PME).

L'action des services de l'État est multiforme (publications, animations, etc.), parfois insuffisamment articulée sur le terrain ou encore mal définie.

L'ANSSI met en ligne et en accès gratuit un grand nombre de publications pour diffuser la culture nécessaire à la maîtrise des risques de cybersécurité ; elle a publié 123 guides techniques de 2015 à 2023. Avec l'outil en ligne *MonAideCyber* (MAC), elle permet des

[143] Le Service de l'information stratégique et de la sécurité économiques (SISSE), service à compétence nationale rattaché à la direction générale des entreprises (DGE) exerce des missions de veille et de mise en cohérence des travaux ministériels en matière de sécurité économique.

diagnostics rapides et gratuits sur la sécurité des systèmes d'information des TPE / PME. Cet outil a été adopté *in fine* par la gendarmerie nationale qui avait pourtant, elle aussi, développé un outil diagnostic, *DIAGnostic Opérationnel NationaL Cyber, Diagonal,* visant un même public. La direction générale des entreprises développe également différentes initiatives pour accompagner la transformation numérique des TPE / PME, notamment dans la fonction de sécurisation des systèmes d'information. Des dispositifs de formation sont proposés dans le cadre de France Num[144], afin d'accompagner les TPE dans leurs démarches de cybersécurisation et 2 000 TPE ont ainsi été sensibilisées aux enjeux de la cybersécurité, depuis deux ans. De manière plus ciblée, la DGE a conçu, en 2023, en collaboration avec l'ANSSI et le SGPI, le dispositif *CyberPME*. Il recouvre un parcours en deux étapes : réalisation d'un diagnostic du système d'information de l'entreprise et définition d'un plan de remédiation afin de permettre une montée en maturité cyber ; appui-conseil afin d'identifier les solutions adaptées et appui financier dans l'acquisition de solutions industrielles et prestations de consulting cyber au travers d'un cofinancement public. Les bénéficiaires doivent être accompagnés par un expert désigné par Bpifrance. L'ambition est d'accompagner 750 entreprises d'ici 18 à 24 mois et, au-delà, d'établir un modèle de référence dans l'accompagnement des PME, à l'image des parcours cyber dont ont bénéficié des collectivités territoriales et des établissements de santé dans le cadre du plan France Relance. Ce référentiel a vocation à orienter les actions des régions et des chambres des commerce et d'industrie destinées à préparer les entreprises à la mise en œuvre de la directive NIS 2.

De fait, le foisonnement d'initiatives gagnerait à être rendu plus lisible pour les petites entreprises mal armées pour s'orienter dans les aides qui leur sont proposées. Récemment, en parallèle du travail réglementaire conduit dans le cadre de la transposition de la directive NIS 2, l'ANSSI a lancé un groupe de travail avec la DGE pour clarifier la stratégie d'orientation des programmes d'aide à la montée en maturité cyber et proposer une méthode pour aligner ces programmes (existants et futurs) avec le référentiel NIS 2. Il s'agit de permettre à toute entité, y compris non régulée, de s'engager dans une démarche de sécurisation adaptée à son niveau et son besoin de cybersécurité.

4.2.3.3 Un dispositif de labellisation, à renforcer

L'ANSSI a mis en place un dispositif de qualification des solutions de cybersécurité – produits ou services (cf. *supra*). En pratique, compte tenu de leur coût, le recours à ces produits et services qualifiés s'adresse aux utilisateurs du « haut du spectre ». L'ANSSI a donc mis à disposition en 2023 une solution en ligne et gratuite « MonAideCyber », destinée à soutenir les entités publiques, associatives et privées, dans une démarche progressive de sécurisation. Elle offre un diagnostic de sécurité cyber gratuit, le soutien d'une communauté d'aidants volontaires, formés gratuitement à cette fin par l'ANSSI, un aiguillage éventuel subséquent vers des dispositifs et des tiers de confiance.

[144] France Num est l'initiative gouvernementale pour la transformation numérique des TPE/PME, pilotée par la Direction générale des entreprises, en collaboration avec Régions de France, l'ensemble des régions et certaines organisations professionnelles. Dans ce cadre, sont proposés aux TPE / PME, des diagnostics numériques et des formations gratuites ; le site internet valorise les bonnes pratiques et référence les aides financières en faveur de la numérisation.

Le label « ExpertCyber » a été développé par *cybermalveillance.gouv.fr* (GIP Acyma), en partenariat avec les principaux syndicats professionnels du secteur), France Assureurs et le soutien de l'AFNOR. Il vise à reconnaître la qualité et l'expertise de professionnels en sécurité informatique ayant démontré un niveau de compétences techniques et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Un annuaire des professionnels labellisés « ExpertCyber » est disponible sur la plateforme et il liste plus de 200 prestataires. Par ailleurs, plus de 1000 professionnels en cybersécurité sont référencés sur l'ensemble du territoire par le GIP Acyma.

D'autres initiatives sont à l'œuvre : la région Île-de-France, par exemple, en plus du CSIRT régional, a monté des marchés avec des prestataires experts, certifiés par l'ANSSI, ouverts aux autres collectivités territoriales franciliennes, de manière à obtenir des prestations aux meilleurs coûts.

En revanche, si la loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public a mis en place un cyberscore de ces entités, qui devait entrer en vigueur le 1er octobre 2023, le cyberscore n'est pas mis en œuvre. Ni le décret définissant les seuils d'activité entraînant l'assujettissement à cette procédure, ni l'arrêté précisant les critères pris en compte par l'audit ne sont parus. Parallèlement la réglementation européenne en la matière a été sensiblement renforcée par le *Digital Services Act* (DSA), applicable depuis le 17 février 2024 et cette évolution réglementaire pose la question de la pertinence du dispositif de cyberscore prévu.

Ces processus de labellisation de prestataires locaux de services, permettant d'établir un niveau de confiance minimal, est donc mis en place sans cohérence et non sans interrogations quant à la robustesse effective des produits ou des prestataires référencés. Il serait nécessaire de construire un cadre de référencement, par concertation entre l'ANSSI, le GIP Acyma et les régions, les bénéficiaires potentiels et les entreprises prestataires.

Recommandation n°10. (SGDSN, ANSSI) Établir des critères de labélisation des solutions de cybersécurité répondant aux besoins des petites et moyennes entreprises et collectivités territoriales.

4.3 La constitution nécessaire d'un vivier de ressources humaines

Le développement et la complexification de la menace cyber rendent chaque jour plus urgent le besoin de doter les entreprises et les administrations de personnels formés, qualifiés et compétents en matière de cybersécurité. Or, les tensions sont aigües sur ce segment du marché[145], ainsi que le montre la volonté affichée dans la stratégie d'accélération de cyber de doubler le nombre d'emplois dans la filière.

[145] Cette difficulté de recrutement est constatée également au Royaume-Uni. Dans son rapport publié en janvier 2025, le National Audit Office indique que plus de 50 % des postes étaient vacants dans plusieurs équipes de cybersécurité ministérielles en 2023/2024. De même, en 2022, 32 % des postes au sein du gouvernement central étaient vacants ou occupés par du personnel temporaire dont le coût est plus que le double des agents permanents.

La réflexion en matière de ressources humaines se décline en trois volets : renforcement de la capacité à répondre à des crises majeures au niveau national, attractivité des emplois au sein de la fonction publique, formation pour constituer une offre de travail conséquente.

4.3.1 Une capacité de réponse à des crises majeures à conforter

Les capacités de l'ANSSI sont limitées, en cas de cyberattaques simultanées, à l'encontre de plusieurs secteurs d'activité ou de plusieurs opérateurs systémiques. Une réflexion est en cours, visant à mobiliser des capacités de réponse au-delà de l'ANSSI.

Elle s'est concrétisée par la signature d'un protocole relatif à la participation des armées au renfort capacitaire de la cyberdéfense en contexte de crise, le 29 mars 2024. Ce document définit les conditions d'une coopération entre l'ANSSI, d'une part, le commandement de la cyberdéfense (COMCYBER) au sein du ministère des armées, en charge de la cyberdéfense dans le périmètre de ce ministère (hors direction générale de la sécurité extérieure et direction du renseignement et de la sécurité de la défense), d'autre part. Il s'agit donc d'un renforcement capacitaire sur le plan strictement défensif. Il définit, de manière très opérationnelle, les modalités de la demande de concours formulée par l'ANSSI, et de soutien apporté par le COMCYBER (état-major des armées). Il règle tous les éléments de procédure et de répartition des coûts induits. Le COMCYBER peut donc être amené *« à soutenir l'ANSSI dans ses missions de cyberdéfense sur l'ensemble du territoire de la République française* ».

Un protocole portant sur le même objet a été signé avant les Jeux olympiques et paralympiques de Paris 2024 avec le ministère de l'intérieur qui dispose de forces importantes en matière de cybersécurité.

Si ce renforcement capacitaire est intéressant, il pourrait être utile de prolonger la réflexion dans deux directions.

La première consisterait à étendre encore la mobilisation de forces, dans le reste du secteur public au fur et à mesure de la montée en compétence des équipes chargées de la cybersécurité, mais également en définissant les conditions dans lesquelles les forces disponibles dans le secteur privé pourraient, le cas échéant, être appelées à contribuer à la cybersécurité. Cette dernière démarche existe déjà dans le domaine de la défense et il convient de s'assurer que les vecteurs contractuels existants et le régime général des réquisitions trouveraient à s'appliquer, s'agissant de la cybersécurité civile.

Un autre axe de réflexion pourrait conduire à renforcer la capacité de réponse de la France aux demandes d'assistance des pays partenaires[146], afin de renforcer la résilience collective et de conforter l'influence française dans le cyberespace.

[146] Comme ce fut le cas, par exemple, du Monténégro lors de l'attaque massive qui l'a visé en août 2022.

4.3.2 Une nécessaire vigilance de l'État sur la gestion de ses ressources humaines

4.3.2.1 Une problématique commune à l'ensemble de la filière numérique publique

En matière de ressources humaines, le secteur de la cybersécurité connaît des problématiques comparables à celles déjà relevées pour l'ensemble de la filière numérique publique, notamment dans le rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique. Un rapport de janvier 2023 sur les ressources humaines de l'État dans le numérique[147] chiffrait ainsi à 130 les recrutements annuels pendant cinq ans en matière de cybersécurité (non compris les besoins en matière de lutte contre les criminalités numériques et pour le renseignement dans l'espace numérique) nécessaires à la bonne marche des services de l'État (sur un total de 2500 pour l'ensemble des fonctions numériques).

Un référentiel de rémunération pour les métiers numériques a été élaboré et déployé par la DINUM pour les contractuels du numérique public. S'il a fortement réduit l'écart de rémunération qui pouvait exister pour ces contractuels au sein de la fonction publique, atténuant ainsi la concurrence entre les administrations, il ne règle pas la disparité de rémunération entre les secteurs public et privé. Il convient par ailleurs de relever qu'en raison des contraintes budgétaires de l'État et des arbitrages effectués par les ministères, il est diversement, voire difficilement, appliqué selon les administrations.

Référentiel de politique salariale de la filière numérique

Le référentiel cadre la politique salariale de 55 métiers de la filière numérique.

Six métiers sont explicitement orientés vers la sécurité numérique : analyste en détection d'intrusions ; analyste en traitement d'incidents informatiques ; auditeur en sécurité des systèmes d'information ; expert méthode et outils / qualité / sécurité ; pilote en détection d'intrusion ; responsable sécurité des systèmes d'information (RSSI).

Globalement, les emplois en cybersécurité sont situés dans la partie haute du spectre des rémunérations, notamment pour les deux derniers.

S'agissant des agents titulaires du numérique public, l'opportunité de leur proposer des formations et des certifications dont l'obtention ouvrirait droit à des primes spécifiques pourrait, selon la DINUM, être utilement étudiée en lien avec la DGAFP.

Les principaux problèmes auxquels se heurte la politique de cybersécurité sont ainsi la rotation forte dans l'emploi, les vacances de poste et le recours massif à des contractuels, parfois à des prestataires de service, pour pourvoir les emplois.

L'ANSSI elle-même enregistre un fort déséquilibre entre titulaires et contractuels, les seconds représentant 83 % des 622 agents fin 2023.

Sa forte visibilité dans le domaine de la sécurité numérique lui permet d'attirer de nombreux talents, même si des tensions apparaissent pour des emplois hyperspécialisés. Pour pallier ces difficultés naissantes, deux chargés de recrutement supplémentaires ont été

[147] Les ressources humaines de l'État dans le numérique - Inspection générale des finances et Conseil général de l'économie de l'industrie, de l'énergie et des technologies, janvier 2023.

embauchés. Par ailleurs, si la grille DINUM pour les emplois de sécurité numérique est prise en référence par l'ANSSI mais difficilement appliquée pour raisons budgétaires, des primes ont cependant été octroyées en 2022 pour éviter un trop grand décrochage avec le secteur privé. Enfin, la gestion prévisionnelle des emplois et des carrières est en cours de structuration au sein de l'ANSSI.

4.3.2.2 Une attention particulière à porter sur les mouvements de personnel au sein de l'ANSSI

Jusqu'au démarrage du chantier GPEC, l'ANSSI promouvait « *un essaimage de ses talents comme autant de "missi dominici" des bonnes pratiques cyber dans l'écosystème* ». Ces échanges avec l'écosystème permettent également, en contrepartie, d'attirer les compétences, un passage par l'ANSSI conférant une forte légitimité dans la sphère de la sécurité numérique.

L'aspect déontologique est traité par l'ANSSI et le SGDSN, employeur des agents de l'ensemble des directions qui lui sont rattachées, conformément à la réglementation en vigueur. Dans le cadre des départs (démission ou création d'entreprise), un premier contrôle est réalisé par la hiérarchie de l'agent, puis par la direction des ressources humaines (DRH) de l'ANSSI, et enfin par le service de l'administration générale (SAG) du SGDSN pour examen. C'est via le SAG qu'est réalisée la saisine éventuelle du déontologue, qui, pour le SGDSN, est le référent déontologue des services du Premier ministre (SPM).

Le SGDSN indique que sa saisine se limite aux seules situations complexes et qu'« *en l'état, il n'a pas été saisi récemment sur une situation relative à un agent ANSSI* ».

Cette absence de saisine du déontologue est étonnante, s'agissant de contractuels de haut niveau, experts dans des domaines stratégiques, susceptibles de connaître des informations sensibles.

Si, dans le cadre de la procédure de recrutement, la DRH de l'ANSSI rappelle à l'agent son obligation d'informer l'agence de ses initiatives d'emploi sur une période de trois ans, après la cessation de ses fonctions à l'ANSSI, dans les faits, aucun suivi n'est réalisé. Les réserves éventuelles et/ou des précautions à prendre dans ses futures fonctions peuvent être indiquées à l'agent oralement mais elles ne sont pas formalisées officiellement. Même si ce cadre déontologique est inscrit, pour les agents contractuels, dans le contrat que l'agent signe à sa prise de fonction, l'absence de réserves officielles et de saisine systématique des commissions de déontologie compétentes ou de la haute autorité pour la transparence de la vie publique (HATVP), en sortie de poste ne permet pas, à ce jour, d'assurer la parfaite sécurité des mouvements sortants.

L'ANSSI prévoit de mettre en place différentes sessions de sensibilisation ou de formations en matière de déontologie et d'élaborer un document précisant le cadre des interactions de ses agents avec des partenaires privés. Il est prévu également que le répertoire des compétences managériales du « manager ANSSI », en cours d'élaboration (le démarrage des travaux a eu lieu en avril 2024), intègre les spécificités liées aux enjeux de déontologie et de préservation des conflits d'intérêts ainsi que du *« droit d'en connaître* ».

Des mesures efficaces devront effectivement être mises en place rapidement.

4.3.3 Un axe formation pris en compte de différentes manières

La constitution d'un vivier de ressources humaines suffisant est une préoccupation réelle, prise en compte dans les multiples activités de l'ANSSI ; notamment une activité de formation au profit des agents des trois fonctions publiques, des OIV et des OSE, dont les modalités de réalisation méritent d'être revues, et un rôle de régulateur, en labellisant des formations cyber, qui devra être étendu et renforcé pour assurer un volume et une qualité des formations répondant aux besoins du secteur.

4.3.3.1 Des actions de sensibilisation aux risques cyber visant un large public

L'ANSSI s'associe à des campagnes de sensibilisation, comme le *Cybermoi/s*, une campagne nationale de sensibilisation aux usages du numérique, qui donne chaque octobre des clés et recommandations à l'ensemble de la population pour mieux se protéger. Elle a également co-construit la campagne *DemainSpécialisteCyber*, qui valorisait la cybersécurité et ses métiers auprès des jeunes et de leurs enseignants, avec le ministère de l'éducation nationale et le Campus Cyber. Le dispositif *CyberEnJeux*, intégré à la campagne, a ainsi permis de former près de 100 000 élèves à la cybersécurité grâce à la création de jeux de société.

Elle mène, en outre, des actions en direction du grand public et notamment mis en place une formation en ligne (Massive Open Online Courses - MOOC), « SecNumacadémie ». Depuis son lancement en 2017, *SecNumacadémie* a formé 257 706 personnes, 55 682 d'entre elles ayant effectué le parcours complet avec succès.

4.3.3.2 Des formations réalisées par l'ANSSI à adapter aux contraintes des administrations

Au travers de son centre de formation pour la sécurité des systèmes d'information (CFSSI), au sein de la sous-direction de l'expertise, l'ANSSI propose 29 formations courtes, ouvertes gratuitement aux agents publics et, depuis 2020, aux personnels des OIV et des OSE. Leur durée varie entre une journée et quatre semaines.

Après deux années bousculées par la crise Covid et le déménagement du centre de formations dans les nouveaux locaux du Campus cyber, en 2022, le CFSSI a enregistré un nombre de candidatures grandissant, issues de nouveaux secteurs d'activité (santé, agriculture, transition écologique, etc.). Le nombre de personnes formées a progressé : elles étaient 1 157 en 2022, 1 644 en 2023 (+ 42,1 %) mais le CFSSI peine cependant à répondre à la demande L'augmentation de l'offre apparaît comme une nécessité incontournable.

À ces formations courtes s'ajoute une formation longue d'un an, gratuite, permettant d'accéder au titre d'« expert en sécurité des systèmes d'information » (ESSI), de niveau 7 (équivalent Bac+5), enregistré au répertoire national des certifications professionnelles (RNCP, nouvellement France Compétences). Alors que la formation peut accueillir, chaque année, une dizaine d'agents publics, 12 candidats ont suivi ce cursus lors de la promotion 2022-2023, mais seulement cinq en 2023-2024.

Les difficultés de recrutement au sein de cette formation sont principalement liées aux réticences des ministères à « détacher » une partie de leur personnel pendant une longue

période. Le CFSSI travaille aujourd'hui à une plus grande promotion de cette formation en direction des différents ministères. Il pourrait être envisagé d'introduire, dans les conventions signées avec chaque ministère, un volet formation, posant une base pluriannuelle des besoins de formation (courtes et longues des ministères), après étude dans chaque ministère des profils à former, à décliner annuellement en fonction de priorités et de la réalité des disponibilités des agents.

4.3.3.3 La politique de labellisation des formations de l'ANSSI

Afin d'aider à l'émergence d'une société de confiance numérique, l'ANSSI a créé le label « SecNumedu » pour les formations spécialisées en sécurité informatique. Pour être labellisées, les formations doivent respecter une charte et des critères définis par l'ANSSI en lien avec les acteurs de l'écosystème cyber. À ce jour, 65 formations ont une labellisation « SecNumedu » en cours de validité. Elle recouvre 32 formations d'écoles d'ingénieur, une formation d'ingénieur de spécialisation, deux licences, dix licences professionnelles, huit mastères, six mastères spécialisés, six titres RNCP de niveau 7.

L'ANSSI propose également un programme de labellisation pour les formations continues et a délivré 36 labels « SecNumedu-FC » : cinq formations sur le thème « Cybersécurité des systèmes industriels » ; quatre formations sur le thème « Méthode EBIOS-RM » ; seize formations sur le thème « Référent cybersécurité pour les TPE/PME » ; onze titres référencés au répertoire national des certifications professionnelles (RNCP).

Ces références restent limitées et ne permettent pas d'obtenir une visibilité totale de l'ensemble des offres de formations proposées en cybersécurité en France. En effet, le label « SecNumedu », ne concerne que les formations de niveau supérieur au Bac+2/3 (DUT/BUT, licence professionnelle, master, mastère spécialisé, cursus d'écoles d'ingénieurs, etc.). En ce qui concerne les formations de niveau inférieur (Bac-Bac+2/3), l'ANSSI ne possède pas de visibilité. Quant à l'offre de formation continue, seules les formations référencées par France Compétences (anciennement répertoire national des certifications professionnelles) sont éligibles au label « SecNumedu-FC », ce qui limite d'autant le catalogue des formations labellisables.

Si l'ANSSI a labellisé récemment des formations spécifiques : méthode collaborative d'analyse des risques, sécurité des systèmes industriels ou encore sécurité des TPE/PME, en développant des cahiers des charges adaptés, cette démarche d'adéquation aux besoins doit être confortée et étendue à d'autres sujets (gestion de crise par exemple, remédiation, ou encore passage à NIS 2 notamment).

De manière plus générale, les études menées sur les besoins des employeurs montrent qu'il est nécessaire de former plus « rapidement » et « massivement » les jeunes dans ce domaine[148] et le recours à des formations plus courtes « Bac+2/Bac+3 » et à l'alternance semble mieux correspondre aux besoins de recrutement actuels en cybersécurité. Ces besoins doivent guider l'offre de formation et un travail d'identification et d'évaluation de ces offres doit être

[148] Les besoins en personnel formé sont estimés à plus de 15 000 postes en France par le groupe de travail sur la formation du Campus cyber (cf. référentiel de compétences des métiers de la cybersécurité – groupe de travail sur la formation – Campus cyber 7 février 2023) et à 17 000 par l'ANSSI.

conduit, parallèlement à un effort d'orientation des candidats potentiels et d'articulation entre les offres de l'État (CFSSI, ministères, etc.) et les offres privées. À cet égard, la DINUM précise que les besoins de formation, bien identifiés dans le cadre du développement du Campus du numérique public, constituent une opportunité de coconstruire une offre encore plus large en matière cybersécurité, en lien étroit avec le CFSSI de l'ANSSI.

Recommandation n°11. (SGDSN, ANSSI) Adapter l'offre interne de formation aux besoins des organismes régulés et développer la fonction d'observation et d'orientation de l'offre de formation en cybersécurité.

CONCLUSION INTERMÉDIAIRE

La lutte contre les cybermenaces, outre la réponse aux agressions, a été traduite par le renforcement des services de l'État et l'accompagnement de l'écosystème cyber.

Alors que la politique de sécurité des systèmes d'information de l'État date de 2014, l'organisation de la gouvernance interne a été restructurée à l'été 2021 dans le but de renforcer la sécurisation des systèmes d'information de l'État. À défaut de sanctions, comme celles applicables aux dirigeants des opérateurs d'importance vitale, il apparaît nécessaire de fixer des objectifs clairs aux dirigeants d'administration, dans leur lettre de mission, concernant l'homologation des systèmes d'information, pour garantir la vigilance nécessaire en la matière.

Par ailleurs, la mise en place de dispositifs de prévention des menaces a procédé de financements exceptionnels. S'ils ont effectivement permis une nette amélioration de la résilience des systèmes d'information de l'État, la nécessité d'un renforcement des performances et d'une adaptation continue face aux mutations des menaces implique de faire entrer la cybersécurité dans une programmation pluriannuelle au sein de chaque ministère, sur la base d'une contractualisation avec le SGDSN.

Quant à l'accompagnement de l'écosystème, il a été concrétisé dans des « outils » emblématiques comme le Campus cyber, efficient comme le GIP Acyma, mais sans définir précisément leurs missions ni leur financement pérenne. Il convient désormais d'élaborer leur modèle économique, en phase avec les besoins du secteur. Par ailleurs, des dispositifs de soutien aux entités les plus fragiles ont été créés par accumulation. Il apparaît nécessaire de les articuler pour les rendre plus lisibles. Un cadre de labellisation des produits et de solutions de cybersécurité pour les entités moyennes ou petites doit être structuré pour faciliter la transparence du marché. Une démarche semblable doit prévaloir en matière de formation pour faciliter l'émergence d'un vivier de ressources humaines nécessaire pour assurer la cybersécurité de l'État et de la Nation.

CONCLUSION

La France s'est dotée dès 2009 d'un dispositif de lutte contre les cybermenaces et a développé en la matière une expertise solide. Elle a intégré très rapidement la cybersécurité dans sa politique de défense nationale, conçue sur un périmètre large englobant les opérateurs d'importance vitale pour le bon fonctionnement de la Nation.

Son dispositif a influencé la réglementation européenne, qui, à son tour, impose désormais des mesures de sécurité renforcée face aux mutations des menaces. Celles-ci sont, en effet, plus sophistiquées, hybrides – mêlant espionnage et cybersécurité – et visent des entités jusqu'alors moins sensibles aux enjeux de sécurité et donc moins armées pour s'en défendre.

Ce changement de paradigme a déterminé l'élaboration d'une nouvelle stratégie nationale de cybersécurité. Celle-ci définit une politique publique globale, visant le développement continu de l'expertise et des technologies avancées et le renforcement du pilotage pour, à la fois, répondre aux agressions, conforter la protection des systèmes d'information de l'État et des entités essentielles et importantes, et construire une « société de confiance » cyber.

Si les objectifs stratégiques sont clairement identifiés et axes d'effort clairement tracés, leur traduction dans le secteur public comme la nécessaire acculturation de la société restent à élaborer. Un plan d'actions détaillé, appuyé sur un échéancier précis et une programmation pluriannuelle des ressources, humaines et financières, doit désormais être défini, pour garantir l'effectivité d'un processus continu de sécurité numérique et nécessairement interministériel.

ANNEXES

Annexe n° 1. Sigles utilisés

ACYMA : assistance aux victimes d'actes de cybermalveillance

ANCT : agence nationale de la cohésion des territoires

ANR : agence nationale pour la recherche

ANSSI : agence nationale de la sécurité des systèmes d'information

APE : agence des participations de l'État

AQSSI : autorité qualifiée en sécurité des systèmes d'information

ARCEP : autorité de régulation des communications électroniques, des postes et de la distribution de la presse

ASTAD : atteinte aux systèmes de traitements automatisés de données

BEFTI : brigade d'enquête sur les fraudes aux techniques de l'information de la préfecture de police de Paris

BITD : base industrielle et technologique de défense

BLCC ou BL2C : brigade de lutte contre la cybercriminalité de la préfecture de police de Paris

BOP : budget opérationnel de programme

C3N : centre de lutte contre les criminalités numériques du service central du renseignement criminel de la gendarmerie nationale

C4 : centre de coordination des crises cyber

C4 STRAT : centre de coordination des crises cyber, niveau stratégique

C4 TechOps : centre de coordination des crises cyber, niveau technique opérationnel

CaaS : *cyber-crime-as-a-service*

CAF : caisse d'allocations familiales

CC : critères communs

CCN : compétence concurrente nationale

CDD : contrat à durée déterminée

CDSN : conseil de défense et de sécurité nationale

CECyber : CEntre d'analyse et de regroupement des Cybermenaces du COMCYBER-MI

CEMP : chef d'état-major particulier du président de la République

CERT : *computer emergency response team*

CERT-FR : *computer emergency response team* France

CERT-UE : *computer emergency response team* Union européenne

CESTI : centre d'évaluation de la sécurité des technologies de l'information

CFSSI : centre de formation SSI de l'ANSSI

CIC : cellule interministérielle de crise

CINUS : comité interministériel de pilotage de la sécurité numérique

CJudOps : comité judiciaire opérationnel

CNAM : caisse nationale de l'assurance maladie

CNCS : centre national de commandement stratégique

CNES : centre national d'études spatiales

CNIL : commission nationale de l'informatique et des libertés

CNF-Cyber : centre national de formation cyber

CNRLT : coordonnateur national du renseignement et de la lutte contre le terrorisme

CODIR : comité de direction

Cofrac : comité français d'accréditation

ComCyberGend : commandement de la gendarmerie dans le cyberespace

COMCYBER-MI : commandement dans le cyberespace du ministère de l'intérieur

COSINUS : comité stratégique interministériel de la sécurité numérique

CPF : compte personnel de formation

CPME : confédération des petites et moyennes entreprises

CPP : code de procédure pénale

CSA : *Cyber Security Act* (directive européenne)

CSIA : Comité de surveillance des investissements d'avenir

CSIRT : *computer security incidence response team* ; centre de réponse aux incidents de sécurité numérique

CSN : conseiller à la sécurité numérique

CSPN : certification de sécurité de premier niveau

CTG : centre de transmissions gouvernemental

CyCLONe : *Cyber Crisis Liaison Organisation Network*

DACG : direction des affaires criminelles et des grâces

DAT : division assistance technique (ANSSI))

DCPJ : direction centrale de la police judiciaire

DCS : délégation aux coopérations de sécurité

DCSSI : direction centrale de la sécurité des systèmes d'information

DESC : division écosystèmes, services et coopération

DDoS : *Distributed Denial of Service* (déni de service distribué)

DGA : délégué général pour l'armement ; direction générale de l'armement

DGE : direction générale des entreprises

DGGN : direction générale de la gendarmerie nationale ; directeur général de la gendarmerie nationale

DGPN : direction générale de la police nationale ; directeur général de la police nationale

DGSE : direction générale de la sécurité extérieure

DGSI : direction générale de la sécurité intérieure ; directeur général de la sécurité intérieure

DGT : direction générale du Trésor

DINUM : direction interministérielle, du numérique

DISSE : délégué à l'information stratégique et à la sécurité économiques

DPSIS : délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité

DRIETTS : direction régionale et interdépartementale de l'économie, de l'emploi, du travail et des solidarités

DRSD : direction du renseignement et de la sécurité de la défense

DSA : *Digital Services Act* (UE)

DTC : direction technique des chiffres

EDR : *Endpoint Detection and Response* (solution de détection et de réponse fonctionnant sur les postes de travail)

eIDAS : electronic Identification, Authentication and Trust Services » (« Services électroniques d'identification, d'authentification et de confiance »

ENISA : *European Union Agency for Cybersecurity* (Agence européenne pour la cybersécurité)

ESP : enquête sous pseudonyme

ETI : entreprises de taille intermédiaire

ETL : *ENISA Threat Landscape* -ETL (panorama ENISA de la menace cyber)

ETP : emploi temps plein

FAI : fournisseurs d'accès à Internet

FII : fonds pour l'innovation et l'industrie

FSSI : fonctionnaire de sécurité des systèmes d'information

FSN : fournisseur de services numériques

GCHQ : *Government Communications Headquarters* (UK)

GPEC : gestion prévisionnelle des emplois, des effectifs et des compétences

GIP : groupement d'intérêt public

HFDS : haut fonctionnaire de défense et de sécurité

IA : intelligence artificielle

ICC : investigateur en cybercriminalité

IEF : investissements étrangers en France

IGI : instruction générale interministérielle

INRIA : institut national de recherche en informatique et en automatique

IOCTA : *Internet Organised Crime Threat Assesment*

IOT : *Internet of Things*

IP : *Internet Protocol*

JIRS : juridiction inter-régionales spécialisée

JOP : jeux olympiques et paralympiques

JPS : justice pénale spécialisée de la direction des affaires criminelles et des grâces (DACG)

JUNALCO : juridiction nationale de lutte contre la criminalité organisée

LBDSN : Livre blanc sur la défense et la sécurité nationale

LBSI : Livre blanc de la sécurité intérieure

LCC : lutte contre la cybercriminalité

LII ou L2I : lutte informatique d'influence

LIO : lutte informatique offensive

LION : laboratoires de l'investigation opérationnelle numérique

LOPMI : loi d'orientation et de programmation du ministère de l'intérieur

LPM : loi de programmation militaire

MTECT : **mi**nistère de la transition écologique et de la cohésion des territoires.

MEAE : ministère de l'Europe et des affaires étrangères

MENJS : ministère de l'éducation nationale, de la jeunesse et des sports

MCO : maintien en condition opérationnelle

MCS : maintien en condition de sécurité (d'un système d'information)

MEFSIN : ministère de l'économie, des finances et de la souveraineté industrielle et numérique

MINARM : ministère des armées

MIOM : ministère de l'intérieur et des Outre-mer

MOOC : *Massive Open Online Courses*

NATINF : NATures d'INFractions

NCF : *National Cyber Force* (UK)

NCSC : *National Cyber Security Center* (UK)

NIS : *Network and Information system Security* (directive UE)

NIST : *National Institute of Standards and Technology* (agence américaine)

NTIC : nouvelles technologies de l'information et de la communication

OCE : opérateurs de communications électroniques

OCLCTIC : office central de lutte contre la criminalité liée aux technologies de l'information et de la communication ; service à compétence nationale au sein de la SDLC

OFAC : office anti-cybercriminalité

OFAST : office anti-stupéfiants

OIV : opérateur d'importance vitale

OSE : opérateur de services essentiels

OSIIC : opérateur des systèmes d'information interministériels classifiés

OTAN : Organisation du Traité de l'Atlantique Nord

PASSI : prestataire d'audit de sécurité des systèmes d'information

PDIS : prestataire de détection d'incident de sécurité

PEPR : programmes et équipements prioritaires de recherche

PHAROS : plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements de contenus et comportements en ligne illicites

PIA : Programme d'investissements d'avenir

PICC : primo-intervenants en cybercriminalité

PIV : point d'importance vitale

PME : petites et moyennes entreprises

PNAT : parquet national antiterroriste

PP : préfecture de police de Paris

PRIS : prestataires de réponse aux incidents de sécurité

PSSI-E : politique de sécurité des systèmes d'information de l'État

RAT : *Remote Administration Tool*

REC : résilience des entités critiques

RGPD : règlement général sur la protection des données

RGS : référentiel général de sécurité

RH : ressources humaines

RIE : réseau interministériel de l'État

RIM : réunion interministérielle

RNS : revue nationale stratégique

RSC : revue stratégique de cyberdéfense

RSSI : responsable de la sécurité des systèmes d'information

SAG : service de l'administration générale (SGDSN)

SAIV : sécurité des activités d'importance vitale

SAS : société par action simplifiée

SCN : service à compétence nationale

SDE : sous-direction de l'expertise (ANSSI)

SDLC : sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire

SDN : sous-direction du numérique

SDO : sous-direction des opérations (ANSSI)

SDS : sous-direction de la stratégie (ANSSI)

SEAE : service européen pour l'action extérieure

SGDSN : secrétariat général de la défense et de la sécurité nationale

SGPI : secrétariat général pour l'investissement

SI : systèmes d'information

SPM : services du Premier ministre

SSI : sécurité des systèmes d'information

SSMSI : service statistique ministériel de la sécurité intérieure

STAD : systèmes de traitement automatisé des données

THESEE : plateforme de traitement harmonisé des enquêtes et signalements pour les e-escroqueries

TPE : très petites entreprises

TRL : *Technology Readiness Level*

UE : Union européenne

UGAP : Union des groupements d'achats publics

UNCyber : unité nationale cyber (gendarmerie nationale)

VIGINUM : service de vigilance et de protection contre les ingérences numériques étrangères

Annexe n° 2. Définitions

En matière de cybersécurité, les définitions sont fournies par l'Agence nationale de sécurité des systèmes d'information (ANSSI), complétées par les définitions applicables au ministère des armées ou utilisées par lui, notamment dans un contexte opérationnel[149]. Ces définitions sont reprises dans le Code de la cybersécurité 2024 (2e édition, code Dalloz).

1. Définitions données par l'ANSSI (Source : https://cyber.gouv.fr/glossaire)

Définitions	Publié le 13 Juillet 2022 - Mis à jour le 21 Septembre 2023	Note de l'ANSSI (2023)
Cyberattaque *« action volontaire, offensive et malveillante, menée au travers du cyberespace et destiné à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support ».* *Glossaire interarmées de terminologie opérationnelle (GIATO),*	**Cyberattaque** Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur **intégrité ou à leur confidentialité.** Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée. **Équivalent anglais : *cyber attack, cyberattack***	L'ANSSI identifie quatre grandes familles de cybermenaces : • la cybercriminalité à visée lucrative ; • l'espionnage ; • la déstabilisation ; • le sabotage. Selon la motivation de l'attaquant et le mode opératoire adopté, chaque cyberattaque pourra être associée à l'une de ces menaces.
Cybercriminalité *Elle est constituée des « actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible ».*	**Cybercriminalité** Ensemble des infractions pénales qui sont commises dans le cyberespace. On distingue les infractions intrinsèquement liées aux nouvelles technologies (diffusion de virus, piratage, copie illicite de logiciels ou d'œuvres audiovisuelles, etc.) et celles pour lesquelles le cyberespace n'est qu'un nouveau lieu d'expression et un nouveau vecteur de transmission (apologie du racisme, diffusion de contenus pédophiles, harcèlement, etc.). **Équivalent anglais : *cybercrime***	L'ANSSI parle le plus souvent de cybercriminalité lorsqu'elle est amenée à s'exprimer sur des cyberattaques menées à des fins lucratives (exemple : rançongiciel).

[149] Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés), JORF n° 0219 du 19 septembre 2017, et glossaire interarmées de terminologie opérationnelle.

Définitions	Publié le 13 Juillet 2022 - Mis à jour le 21 Septembre 2023	Note de l'ANSSI (2023)
Cyberdéfense *« Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels ».*	**Cyberdéfense** Ensemble des moyens mis en **place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.** La cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive. **Équivalent anglais : *cyber defence, cyberdefence***	En matière de cyberdéfense, l'ANSSI n'intervient que sur le volet défensif, le volet offensif étant de la responsabilité d'autres acteurs. Dans ce cadre, l'agence développe et structure les capacités de détection de l'État et organise au niveau national l'assistance aux victimes de cyberattaques.
Cyberespace *« Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ».*	**Cyberespace** Espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet. **Équivalent anglais : *cyberspace***	Perçu comme un nouveau territoire, le cyberespace est un espace difficile à définir car il repose sur un ancrage à la fois physique et informationnel.
	Cyberespionnage Ensemble d'actions menées dans le cyberespace consistant à infiltrer, clandestinement ou sous de faux prétextes, les systèmes informatiques d'une organisation ou d'un individu, et à s'emparer de **données pour les exploiter.** Le cyberespionnage se pratique notamment par le biais de logiciels malveillants ou espions, de cyberattaques persistantes, ou en mettant à profit les vulnérabilités des systèmes informatiques. **Équivalent anglais : *cyber espionage, cyber spying***	Le cyberespionnage constitue l'une des menaces les plus redoutées par l'ANSSI. Les auteurs de ces actes recourent le plus souvent à des méthodes très pointues, ils peuvent rester tapis très longtemps dans un système d'information sans jamais se faire repérer. Les conséquences de l'espionnage peuvent être désastreuses pour la ou les organisations qui en sont victimes.
Cybersécurité *« État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou*	**Cybersécurité** État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace. La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un État, par la cyberdéfense.	Il est fréquent de voir les termes ***cybersécurité* et *sécurité numérique* employés tour à tour comme des synonymes.** Pourtant, il est communément accepté que la cybersécurité - à l'image d'autres termes dotés du préfixe ***cyber*** **- renvoie à la sécurité des systèmes d'information tandis que la sécurité numérique renvoie plus**

Définitions	Publié le 13 Juillet 2022 - Mis à jour le 21 Septembre 2023	Note de l'ANSSI (2023)
transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessible ». L'ANSSI précise que la cybersécurité « fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense ».	**Equivalent anglais (GB) : *cybersecurity***	**largement à la sécurité des systèmes et des pratiques numériques. Ainsi, les bonnes pratiques de sécurité numérique sont aussi bien techniques que comportementales.**
	Cyberrésilience « Capacité d'un système d'information à résister à une panne ou une cyberattaque et à revenir à son état initial après l'incident » ou, du moins, à un état de fonctionnement et de sécurité satisfaisant.	
Lutte informatique défensive (LID) *« Dans le cadre des opérations dans le cyberespace, action consistant à surveiller, analyser, détecter et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire les systèmes, réseaux et données. »*		
Lutte informatique offensive (LIO) *« Dans le cadre des opérations dans le cyberespace, action non physique entreprise dans le cyberespace contre des systèmes d'information ou des données pour les perturber, les modifier, les dégrader ou les détruire. »*		
	Filoutage Technique de fraude visant à obtenir des informations confidentielles, telles que des mots	L'ANSSI parle le plus souvent de hameçonnage pour désigner cette pratique. Pour parvenir à leurs fins, les auteurs de ces attaques recourent à des

Définitions	Publié le 13 Juillet 2022 - Mis à jour le 21 Septembre 2023	Note de l'ANSSI (2023)
	de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales. Le terme « hameçonnage » est aussi en usage. **Équivalent anglais : *phishing***	procédés techniques et/ou d'ingénierie sociale.
	Logiciel rançonneur (ou rançongiciel) Logiciel malveillant qui empêche l'accès aux données stockées sur un ordinateur et propose leur récupération contre le paiement d'une rançon. En général, un logiciel rançonneur chiffre les données de l'ordinateur cible en indiquant les instructions de paiement. **Équivalent anglais : *ransomware***	L'ANSSI parle le plus souvent de rançongiciel pour désigner ce type d'attaque. Les rançongiciels font partie des attaques les plus redoutées par l'agence avec une évolution remarquable au cours des dernières années en termes de **sophistication, d'amplitude et de conséquences.**
	Opérateur d'importance vitale (OIV) Personne morale publique ou privée qui gère ou utilise des établissements ou des ouvrages dont la destruction ou même l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité, voire la capacité de survie d'un État, ou mettraient en danger sa population. **Équivalent anglais : *Operator of critical national infrastructures***	L'ANSSI a notamment pour mission d'accompagner les OIV dans la sécurisation de leurs systèmes d'information sensibles.

2. Code de la cybersécurité 2024 – 2e édition, Dalloz - Tous droits réservés

Article 2.1) du règlement (UE) 2019/881 du 17 avril 2019, dit « Cybersecurity Act », qui rassemble dans le vocable cybersécurité : « *les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces* ». Dans le même article, en son point 8), une cybermenace est définie comme « *toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes* ».

Dans le glossaire de l'agence nationale de la sécurité des systèmes d'information (ANSSI), la cybersécurité est un « *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* » (https://www.ssi.gouv.fr/entreprise/glossaire/, consulté le 27 mars 2022). La cybersécurité est donc un résultat qui se mesure après une conjugaison d'actions.

En apparence, parce qu'ils sont parallèles, ces piliers devraient être indépendants. En vérité, il n'en est rien, car ils ont un socle commun : le substrat numérique qui est le siège de la matière première essentielle, les données, qui favorise le partage de l'information, le renseignement d'intérêt cyber et le renseignement d'origine cyber et qui fait appel à des techniques forensiques souvent similaires, notamment à la recherche de la preuve numérique. La sécurité des systèmes d'information (SSI) contribue à la prévention de la cybercriminalité ; elle pénètre dans le champ de la cyberdéfense par le biais des opérateurs d'importance vitale (OIV) et des opérateurs télécom.

3. Journal officiel de la république française n° 0219 du 19 septembre 2017 (Texte 45 sur 69, extraits)

COMMISSION D'ENRICHISSEMENT DE LA LANGUE FRANÇAISE

Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés)
NOR : CTNR1724864K

I. – Termes et définitions

cyberattaque, n.f.

Définition : Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.

Note : Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

(…)

cyberattaque persistante

Définition : Cyberattaque qui met en œuvre des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation.

Note : Une cyberattaque persistante recourt à des techniques furtives qui s'adaptent graduellement aux actions de cyberprotection qu'elle suscite.

(…)

cyberdéfense, n.f.

Définition : Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.

Note : La cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive.

(…)

cyberdéfense militaire

Définition : Ensemble coordonné d'actions défensives et offensives menées dans le cyberespace lors de la planification, de la préparation ou de la conduite d'opérations militaires.

Note : La cyberdéfense militaire s'appuie sur des opérations dans le cyberespace ainsi que sur des actions de renforcement de la cyberrésilience.

(…)

cyberespace, n.m.

Définition : Espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées.

Note :

1. Le cyberespace inclut les opérateurs de services en ligne.
2. On trouve aussi le terme « cybermonde », parfois utilisé dans ce sens.

(…)

cyberprotection, n.f.

Définition : Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité.

Note : La cyberprotection s'appuie notamment sur des mesures prises pour préserver la sécurité des systèmes d'information.

(…)

cyberrenseignement, n.m.

Définition : Ensemble d'actions menées dans le cyberespace consistant à infiltrer les systèmes informatiques d'une organisation et à s'emparer de données pour exploiter, à des fins opérationnelles, les renseignements ainsi recueillis.

Note : On trouve aussi, dans le langage professionnel, le terme « exploitation informatique (EI) ».

(…)

cyberrésilience, n.f.

Définition : Capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, puis à revenir à un état de fonctionnement et de sécurité satisfaisant.

(…)

cybersécurité, n.f.

Définition : État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.

Note : La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un État, par la cyberdéfense.

(…)

lutte informatique défensive

Abréviation : LID.

Définition : Ensemble coordonné d'actions menées par un État, qui consistent à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant.

(…)

lutte informatique offensive

Abréviation : LIO.

Définition : Ensemble coordonné d'actions menées dans le cyberespace par un État contre des systèmes d'information ou de données pour les perturber, les modifier, les dégrader ou les détruire.

(…)

opérateur d'importance vitale

Abréviation : OIV.

Définition : Personne morale publique ou privée qui gère ou utilise des établissements ou des ouvrages dont la destruction ou même l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité, voire la capacité de survie d'un État, ou mettraient en danger sa population.

(…)

opérations dans le cyberespace

Définition : Actions relatives à la lutte informatique défensive, à la lutte informatique offensive et au cyberrenseignement.

Note : Les opérations dans le cyberespace constituent l'une des composantes de la cyberdéfense militaire.

(…)

renseignement intéressant la cyberdéfense militaire

Abréviation : RICM.

Définition : Renseignement qui apporte à la chaîne de commandement opérationnel de la cyberdéfense militaire les informations dont la connaissance est nécessaire pour conduire des opérations dans le cyberespace.

Note : On trouve aussi, dans le langage professionnel, le terme « renseignement d'intérêt cyber (RIC) ».

(…)

Annexe n° 3. Les parcours de sécurité au bénéfice des collectivités territoriales

Le programme a été lancé en 2021 et les dernières actions devraient aboutir mi-2025.

Alors que l'objectif initial était d'accompagner 700 bénéficiaires, environ 950 ont été acceptés. 24 entités ont abandonné en phase préalable. En parallèle, plus de 680 candidatures ont été réorientées vers un service plus adapté à leurs besoins : dispositif d'appel à projet monté dans le même cadre du plan de relance, pour les structures les plus matures, et, pour celles disposant de systèmes d'information de faible ampleur, service des opérateurs publics de service numériques (OPSN) et solutions de cybersécurité mutualisées.

Tableau n° 13 : Nombre et nature des bénéficiaires

Entités bénéficiaires	Nombre
Collectivités territoriales	707[150]
Établissements de santé	133
Établissements publics	106
Total	946*

*Source : ANSSI - les parcours de cybersécurité : rapport d'activité 2023 *978 au 25 avril 2024*

Ces parcours sont destinés à outiller les bénéficiaires pour répondre aux menaces les plus pressantes auxquelles ils sont confrontés. La démarche est à la fois standardisée et personnalisée. Une première étape de pré-diagnostic permet d'établir le niveau de maturité du bénéficiaire.

L'accompagnement proposé ensuite recouvre une phase d'audit standardisée (pack initial) et une phase de mise en œuvre opérationnelle des mesures prioritaires.

[150] Ces parcours de sécurité sont une expérimentation destinée à éprouver une méthodologie sur un périmètre limité. Sans commune mesure avec les 34 945 communes, et les 33 799 communes de plus de 1000 habitants, le nombre de collectivités concernées est, en revanche, commensurable aux 1040 de plus de 10 000 habitants (y compris Paris) auxquels il convient toutefois d'ajouter les départements et régions, voire les intercommunalités.

Tableau n° 14 : Déroulé du programme

Accompagnement		
Cellule Relation Candidats de l'ANSSI	Prestataire accompagnateur : suit les bénéficiaires, soutient les prestataires de terrain, garantit la cohérence globale du dispositif / prestataire de terrain.	
	Sur la base d'une démarche formalisée grâce à des concepts et guides préalablement produits par l'ANSSI (guide d'hygiène ou guide sur les attaques par rançongiciels notamment)	
Durée moyenne : 4 mois	Durée moyenne : 8 mois	Durée moyenne :11 mois. Au-delà de 12 mois, le reste du plan est déployé en autonomie par le bénéficiaire, avec le soutien des délégués territoriaux et sectoriels de l'ANSSI.
Nature des prestations		
	Prestations standardisées : Sensibilisation, audits organisationnels et techniques.	Mise en œuvre des mesures de sécurisation : acquisition et installation de matériels et solutions de cybersécurité, recours à des prestations d'audit et d'expertise.

Source : Cour des comptes d'après ANSSI

Dans son rapport sur les parcours de sécurité, l'ANSSI souligne le « *grand nombre de vulnérabilités* » détectées, ce qui démontre la faiblesse du niveau initial de sécurité des organismes concernés. Les vulnérabilités identifiées lors du diagnostic (Pack initial) relèvent des fondamentaux de la cybersécurité : absence de gestion de l'obsolescence et des mises à jour, absence de politiques de mots de passe, accès administrateurs non centralisés, annuaires non sécurisés, absence d'isolation des sauvegardes, réseaux décloisonnés, messageries exposées, postes de travail non supervisés. Dès la première phase du Parcours, des actions de remédiation immédiate sont menées pour corriger les failles de sécurité les plus urgentes. Quasiment tous les parcours (93 % d'entre eux) comprennent de telles mesures[151].

Un des principaux objectifs des parcours de sécurité réside dans la sensibilisation des équipes dirigeantes des organismes accompagnés – y compris les élus -, de sorte à « *mettre la cybersécurité au cœur des priorités stratégiques* ». 96 % des prestataires de terrain, acteurs du pack initial, ont noté une amélioration de la sensibilité des dirigeants. Des publics spécifiques d'agents sont également visés, du fait de l'exposition aux cybermenaces de leur activité quotidienne : équipes achats et ressources humaines, développeurs, administrateurs et ingénieurs biomédicaux dans les établissements de santé. 6 600 personnes ont ainsi participé à ces campagnes de sensibilisation, réalisées dès la phase initiale des Parcours.

[151] Comme l'inscription au service ADS (Active Directory Security) développé par l'ANSSI (voir note de bas de page *supra*). 828 annuaires sont ainsi suivis par l'ADS dans le cadre du parcours de cybersécurité et le dispositif a permis une amélioration moyenne de 9 % du niveau de sécurité des AD.

Les pack relais, quant à eux, ont conduit à valider plus de 1 900 mesures, pour près de 450 bénéficiaires. La mesure du niveau de vulnérabilité des systèmes d'information[152] face à trois types de menaces - les nuisances quotidiennes, les menaces cybercriminelles et les menaces étatiques - en début et à l'issue de l'accompagnement montre qu'en moyenne les bénéficiaires du parcours sont passés du score D+ à B (sur une échelle de D- à A+). L'amélioration est donc significative, en tous cas en moyenne. Il conviendrait cependant de préciser la cible recherchée, selon la sensibilité des entités concernées et surtout de prévoir les moyens d'optimiser la sécurité des SI en continu.

Or, les parcours de sécurité sont financés par le bénéficiaire de l'accompagnement, en complément de la subvention versée sur crédits du BOP 363 SGDSN. Les dépenses prévisionnelles, par organisme, pour un pack relais sont estimés par l'ANSSI[153] à 86 282 € en moyenne pour une collectivité territoriale ou un établissement public et 150 568 € pour un établissement de santé. L'ANSSI évalue à 123 M€ la commande passée aux fournisseurs, au regard des 90 M€ de subventions accordées, soit 33 M€ de dépenses à la charge des bénéficiaires. La sécurisation a donc un coût pour les entités publiques qu'il convient de prévoir dans leur budget, non seulement en investissement initial mais également sur le long terme et en fonctionnement pour assurer le maintien en condition de sécurité de leur SI. Le cadre normatif de leur budget pourrait prévoir une ligne de compte consacrée à ces opérations.

Au-delà de la sécurisation des bénéficiaires, la démarche a eu un impact positif sur le tissu industriel français de cybersécurité, souligné par les prestataires de terrain questionnés sur ces sujets[154] : 193 prestataires différents ont contribué à la réalisation des packs initiaux, et 215 fournisseurs de solutions et de matériels ont été mobilisés pour les packs relais. Les solutions mises en œuvre dans le cadre des packs relais ont été à 79 % françaises et 15 % européennes.

L'effet levier en faveur des offreurs est donc conforme aux attentes et il convient de souligner l'impact économique de cette forme de politique industrielle.

[152] Dont la méthodologie consiste à évaluer, sur un total de 400 points, 14 thèmes de la cybersécurité relatifs à la gouvernance des SI, la sécurité des réseaux, le niveau de protection des données ou encore la conformité des audits (cf. les parcours de cybersécurité - rapport d'activité 2023).

[153] cf. rapport d'activité 2022 sur les parcours de cybersécurité.

[154] cf. rapport d'activité 2023 sur les parcours de cybersécurité : les prestataires terrain ont estimé à 88 % que les parcours avaient eu un impact positif sur leur activité, à 45 % qu'ils leur avaient permis de renforcer leurs effectifs, et à 61 % de développer une offre similaire à destination d'autres organismes publics et privés.

Annexe n° 4. Principaux dispositifs d'assistance au public en cas de cyber-agression

Nom de la plateforme	Opérateur	Objet	Type de menace	Public visé
Signal-SPAM	Association loi de 1901 regroupant acteurs publics et privés	Signalement	Courrier électronique non sollicité ou malveillant	Grand public
Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (**Pharos**) Créée en 2009	Ministère de l'intérieur (OFAC)	Signalement .	Contenus publics et comportements en ligne illicites.	Grand public
	Disponible en ligne 24/24 et 7j/7 La plateforme a reçu 211 543 signalements en 2023.			
Traitement harmonisé des enquêtes et signalement pour les e-escroqueries (**THESEE**) Lancé le 15 mars 2022	Ministère de l'intérieur (OFAC)	Premier dispositif de dépôt de plainte en ligne pour les victimes d'arnaques en ligne.	E-escroqueries	Tous publics (victimes ou témoins)
	Disponible en ligne 24/24 et 7 jours /7 La plateforme a enregistré 104 439 déclarations en 2023 Cinq types concernés : 1/ « escroquerie aux sentiments » ou « escroquerie à la petite annonce » : création de faux profils sur Internet pour convaincre la victime de remettre des fonds ; 2/ chantage en ligne comportant une demande d'argent ; 3/ « rançongiciel » (ou « ransomware ») : demande de rançon consécutive au chiffrement des données d'un STAD et d'une entrave à son accès (ordinateurs, smartphones, tablettes…) ; 4/ piratage de comptes de courriel ou de profils de réseaux sociaux ; 5/ fraude sur un faux site de vente en ligne.			
Phishing initiative	Orange Cyberdéfense	Signalement	Hameçonnage	Grand public
Plateforme téléphonique « Info escroqueries » Lancée en 2009	Ministère de l'intérieur (POAC)	Information et prévention sur les escroqueries sur internet	Escroqueries en ligne	Grand public
33700	Association française du multimédia mobile (AFMM)	Signalement	SMS indésirables	Grand public
Percev@l Ouvert au public depuis juin 2018	Ministère de l'intérieur	Signalement	Fraude à la carte bancaire (principalement sur internet)	Grand public

	La plateforme a enregistré 259 094 signalements en 2023.			
Assistance de victimes d'actes de cybermalveillance *Cybermalveillance.gouv.fr* Créé en mars 2017	Groupement d'intérêt public	Information, sensibilisation, assistance	Escroquerie et cyberattaque	Grand public, entreprises privées (TPE, PME, ETI), administration, organisme public, collectivités territoriales non régulées
	Plateforme visitée par plus de 3,7 millions de personnes en 2023. Plus de 280 000 demandes d'assistances analysées en 2023.			
« 17 Cyber » 17cyber.gouv.fr Mise en œuvre opérationnelle le 17/12/2024		Information, signalement et assistance	Escroquerie et cyberattaque	Grand public et organismes non régulés
Filtre anti-arnaque	En cours	Assistance	E-arnaques	Professionnels
	Au profit des professionnels assujettis à l'obligation de mise en œuvre du filtre national de cybersécurité au bénéfice de la Direction Générale des Entreprises (DGE)			

Source : Cour des comptes