RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Etat de la prise en compte de la cryptographie post-quantique par les bénéficiaires de l'ANSSI en 2023

SOMMAIRE

SOMMAIRE

INTRODUCTION ____ 3.

1. ETUDE DE L'ANSSI SUR LA TRANSITION POST-QUANTIQUE ____ 4.

2. SYNTHÈSE DE L'ENQUÊTE ____ 5-6.

3. PRINCIPALES RAISONS EXPLIQUANT L'ABSENCE DE PRISE EN COMPTE DE LA MENACE QUANTIQUE PAR LES BÉNÉFICIAIRES ____ 7.

CONCLUSION ____ 8.

Étude de l'ANSSI sur la transition post-quantique

Dans le cadre d'une étude visant à identifier des mesures qui pourront faciliter la transition des organisations vers la cryptographie post-quantique (PQC[1]), l'ANSSI a mené une enquête auprès d'un échantillon[2] de ses bénéficiaires[3]. Les questions posées aux organisations interrogées concernaient la connaissance de la menace quantique et des contremesures pour y répondre, l'état d'avancement d'un éventuel plan de transition et les cas d'usage identifiés, ainsi que les attentes vis-à-vis de l'offre privée et de l'administration, l'ANSSI en particulier.

Après un rappel des enjeux de la transition vers la cryptographie post-quantique, le document présente la synthèse de l'analyse des réponses et les freins majeurs à la transition tels qu'indiqués par les répondants.

Cette enquête s'inscrit dans un travail de long terme de l'ANSSI pour accompagner les acteurs publics et économiques à se préparer à l'arrivée de la menace quantique et notamment faciliter l'émergence de solutions technologies innovantes pour se prémunir contre cette menace.

1. L'acronyme PQC pour Post-Quantum Cryptography est le plus largement adopté dans la communauté scientifique, y compris francophone.

2. Trente-huit bénéficiaires de différents secteurs ont répondu au questionnaire entre juillet et septembre 2023.

3. Le terme « bénéficiaire » désigne dans ce document les entités, privées ou publiques, devant répondre à des exigences règlementaires de gestion de leur cybersécurité comme par exemple les Opérateurs d'Importance Vitale (OIV).

1. Enjeux de la transition post-quantique d'un système d'information

La transition post-quantique concerne en premier lieu la **cryptographie asymétrique**[4], notamment pour les usages en confidentialité et échanges de clé pour se prémunir contre des attaques rétroactives.

Les primitives cryptographiques actuellement déployées (« pré-quantiques ») sont bien maîtrisées par les développeurs en cybersécurité et il en existe de nombreuses implémentations efficaces et robustes, sous forme de bibliothèques commerciales ou libres.

La situation des futurs standards post-quantiques est différente. En effet, seuls quelques spécialistes du domaine maîtrisent complètement ces primitives[5] . Des implémentations efficaces et durcies – qu'elles soient logicielles ou sur plateforme matérielle – vont demander beaucoup de temps et d'efforts. De même, les mécanismes et protocoles qui mettent en œuvre ces nouvelles primitives sont récents et ne jouissent pas du même niveau d'assurance et de confiance dans leur niveau de sécurité.

Ce constat global s'applique autant aux algorithmes d'établissement de clé qu'aux signatures numériques.

[4]. Se référer à l'avis scientifique de l'ANSSI sur la migration vers la cryptographie post-quantique publié en décembre 2023 : https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique.

[5]. Éléments de base pour construire des systèmes cryptographiques capable de résister à des attaques quantiques qui reposent sur des problèmes mathématiques considérés comme complexe à résoudre par un ordinateur quantique.

2. Synthèse de l'enquête

Plus de la moitié des bénéficiaires de l'ANSSI interrogés semble dès aujourd'hui être à risque vis-à-vis de la menace de l'ordinateur quantique. En cause : leur recours à des pratiques vulnérables aux attaques rétroactives, telles que l'usage de VPN pour transmettre des informations sensibles dont la confidentialité doit être assurée pour une durée supérieure à 10 ans, ou l'exploitation de certificats dont la durée de vie excède également 10 ans.

La grande majorité des bénéficiaires a connaissance de cette menace quantique d'un point de vue théorique ; mais l'impact concret de celle-ci sur leurs systèmes d'information ne leur est pas connu.

Ceci explique que les travaux d'analyse des risques liés à la menace quantique ne sont ni engagés, ni planifiés, ni budgétés pour la quasi-totalité des bénéficiaires. **Aucun plan de transition post-quantique n'existe.** Les RSSI consultés n'ont pas une idée précise de la date à laquelle leurs systèmes d'information devront avoir migré ni le temps qu'une telle transition pourrait prendre. Les cas d'usage prioritaires – c'est-à-dire urgents – ne sont pas non plus identifiés et ne peuvent donc être pris en compte.

L'enquête fait très nettement ressortir **un fort besoin d'accompagnement de ces entités par des prestataires externes**, tant pour les travaux préparatoires d'élaboration d'un plan de transition (analyse de risque quantique, identification des cas d'usages prioritaires, inventaire des actifs cryptographiques, classification des données) que pour accompagner la transition elle-même (formation, conseil, transformation, suivi des fournisseurs, mise à jour des applications métier, etc.).

Pour ce faire, les équipes en charge des risques cyber **ont besoin de moyens financiers et humains**. Cela passe par un nécessaire **soutien des Directions générales des bénéficiaires** et donc l'appropriation du sujet par les décideurs au plus haut niveau.

Par ailleurs, les bénéficiaires ont de fortes attentes concernant l'implication de l'ANSSI dans la transition post-quantique. L'Agence est ainsi attendue dans un rôle de régulateur et tiers de confiance, de conseil et d'expertise technique, de pédagogie (sensibilisation et formation), ou encore dans un rôle de législateur.

Partant de ce constat, les équipes de l'ANSSI rappellent que les bénéficiaires ont pleinement leur rôle à jouer dans cette transition. Il est en effet nécessaire que les organisations s'approprient le sujet, mettent en place les ressources et travaux d'analyse nécessaires : recensement des actifs cryptographiques, capacité de crypto-agilité et analyse d'impacts notamment.

L'écosystème ne s'est pas encore réellement emparé du sujet et force est de constater que chacun compte sur les autres pour avancer.

3. Principales raisons expliquant l'absence de prise en compte de la menace quantique par les bénéficiaires

Au-delà des explications fournies par les entités consultées, le travail d'analyse de leurs réponses fait ressortir 4 raisons majeures à la passivité observée face à la menace :

A. Mauvaise compréhension des enjeux et de l'agenda quantique. C'est la raison principale qui ressort de cette enquête ; tous les autres freins ne sont que des conséquences de cet état de fait. Les bénéficiaires ne se sont pas encore emparés du sujet post-quantique car ils n'ont pas clairement identifié ses enjeux. À leur décharge, aucune communication formelle d'une date ou d'un planning incitatif ou contraignant n'a été faite en France, pour le moment.

B. Manque de moyens financiers et humains. Tant que le risque n'aura pas été pleinement matérialisé dans l'esprit des organisations, traiter la menace quantique restera à un niveau de priorité très bas, et aucun moyen ne sera accordé pour traiter ce « non sujet ».

C. Absence d'offre de services d'accompagnement à la transition post-quantique. Les acheteurs et les RSSI ne sont pas sollicités par leurs commerciaux habituels pour acheter des prestations relatives à la menace quantique, ce qui, dans le cas contraire, pourrait les inciter à considérer le sujet comme étant d'actualité.

D. Absence d'obligation réglementaire (pour les entités régulées). C'est – malheureusement – parfois le seul levier efficace, quand les autres approches ont échoué, pour faire évoluer une situation bloquée. Au-delà de l'aspect coercitif, l'existence d'une réglementation rend concrète une menace et priorise sa prise en compte par les entités régulées concernées. Par ailleurs, l'effet d'entrainement sur le reste de l'écosystème n'est pas à négliger.

CONCLUSION

CONCLUSION

Cette enquête auprès des bénéficiaires de l'ANSSI confirme les constats des deux enquêtes menées auprès des prestataires de services et des fournisseurs de solutions[6] : les organisations ne sont pas sensibilisées à la menace quantique et à son agenda, et manquent de moyens financiers et humains pour prendre en compte ces enjeux. Cela explique l'absence de demande de solutions et prestations post-quantiques.

Face à ces observations, l'ANSSI rappelle l'importance de démarrer sans tarder les actions préparatoires à la transition post-quantique, dans tout type d'organisations. Il est important que chaque organisation évalue son niveau de risque réel vis-à-vis de la menace quantique et élabore son plan de transition. Certaines actions devront être mises en œuvre sans délai et d'autres, progressivement, sur les années à venir.

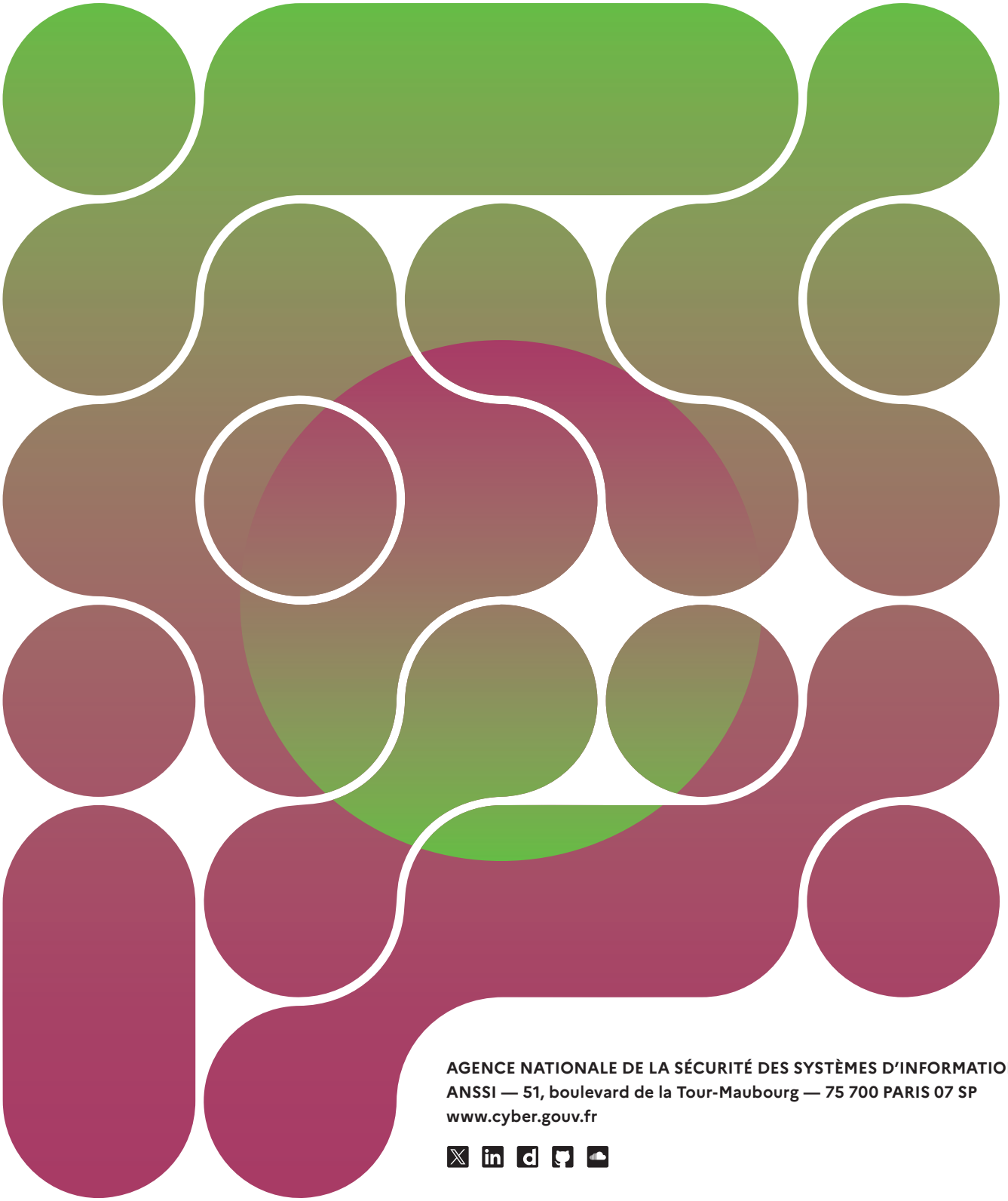
L'ANSSI est d'ores et déjà active sur le chantier de la migration et agit à court terme pour :

- Poursuivre et approfondir sa connaissance de l'offre et de ses évolutions ;
- Soutenir l'émergence de produits et solutions permettant de faciliter la transition vers la cryptographie post-quantique[7] ;
- Être actrice d'une bonne coopération avec ses partenaires, notamment européens[8].

[6]. Les études de l'ANSSI sont disponibles ici : https://cyber.gouv.fr/actualites/anssi-partage-deux-etudes-de-marche-sur-la-cryptographie-post-quantique-menees-aupres

[7]. L'axe 4 de l'appel à projets « Technologies Critiques 4 » a pour thème est la protection des données, se concentre sur les outils d'aide à la transition (Appel à projets « Développement de technologies innovantes critiques 4ème édition » | Bpifrance).

[8]. Voir la note Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography (Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography | ANSSI).



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