# CRYPTO POST-QUANTIQUE

## 2026 : l'année du tournant stratégique

THEGREENBOW

CRYPTO POST-QUANTIQUE
2026 : l'année du tournant stratégique
Note stratégique.

# LA TRANSITION S'ACCÉLÈRE : LE TEMPS EST À L'ACTION

L'avènement de l'informatique quantique représente la menace cryptographique la plus structurelle depuis l'invention d'Internet. Les algorithmes qui protègent aujourd'hui les communications gouvernementales, les transactions financières, les données de santé et les infrastructures critiques pourraient être rendus caducs dans un horizon de cinq à dix ans. La stratégie d'attaque « Harvest Now, Decrypt Later – collecter aujourd'hui pour déchiffrer demain – est déjà à l'œuvre depuis plusieurs années. La migration vers la cryptographie post-quantique n'est plus une option : c'est une urgence stratégique. Le chemin sera long, mais deux bonnes nouvelles : les acteurs sont mobilisés pour guider, accompagner cette transition et les moyens sont disponibles !

***Mathieu Isaïa***
***Directeur général TheGreenBow***

# L'ÉTAT RÉEL DE LA MENACE : AU-DELÀ DES CHIFFRES DE QUBITS

Le débat public sur le Q-Day souffre d'une confusion persistante entre qubits physiques et qubits logiques. Les annonces d'IBM (1 000+ qubits) ou de Google (Willow, 105 qubits physiques en 2024) sont réelles mais ne signifient pas que la capacité de casser RSA-2048 est imminente. Les estimations sérieuses, dont celles du NIST et de l'ENISA, évaluent le besoin à plusieurs millions de qubits physiques de haute qualité pour atteindre ce seuil, en raison du coût en redondance de la correction d'erreurs quantiques. Willow a démontré une réduction exponentielle des erreurs à mesure que le nombre de qubits augmente — c'est la démonstration de principe qui change la donne, pas encore la machine opérationnelle. Le Gouvernement français a annoncé, le 22 mai 2026, un investissement d'un milliard d'euros pour accélérer le développement d'une filière quantique française et européenne d'ici à 2030. Le programme PROQCIMA, dédié au développement d'un ordinateur quantique de conception française, verra également son ambition renforcée avec un objectif porté à 1 024 qubits logiques à horizon 2032 et 2 048 en 2035 : ces jalons sont cohérents avec une fenêtre de vulnérabilité réelle autour de 2033-2038 pour les systèmes les mieux financés.

**Ce qui importe pour les décideurs n'est pas la date exacte du Q-Day mais le delta entre ce délai et le temps nécessaire à leur propre migration.** Pour la plupart des systèmes d'information complexes — en particulier dans la défense, les infrastructures critiques et la finance —, ce delta est déjà négatif. Il est clair que la problématique majeure est le temps nécessaire de migration et la masse de systèmes interconnectés à migrer en même temps. **Les deux concepts d'hybridation et de crypto-agilité prennent tout leur sens.**

La migration cryptographique d'un système d'information complexe prend en moyenne 5 à 10 ans. Les systèmes d'armes, les infrastructures critiques, les plateformes bancaires et les réseaux de santé ont des cycles de vie de 15 à 30 ans. Attendre d'avoir la certitude de l'arrivée de l'ordinateur quantique serait une faute stratégique irréversible.

La stratégie HNDL (*Harvest Now, Decrypt Later*) change fondamentalement le calcul temporel. Elle signifie que la compromission ne se produit pas au Q-Day mais en amont, lors de la collecte. Les données dont la confidentialité doit tenir 10 ans ou plus sont donc déjà sous menace active. Vincent Strubel, directeur général de l'ANSSI l'a formulé sans ambiguïté : *« ce n'est plus théorique »*. Les flux diplomatiques, les échanges interopérateurs de défense, les données génomiques et les registres industriels stratégiques doivent être traités comme potentiellement collectés aujourd'hui par des acteurs disposant des capacités de stockage nécessaires — capacités que la Chine, la Russie et la NSA possèdent indiscutablement.

CHAPITRE II

# ÉTAT DE L'ART : LES RÉPONSES NORMATIVES ET TECHNOLOGIQUES

## I. La standardisation du NIST : un tournant historique

En août 2024, le National Institute of Standards and Technology (NIST) américain a finalisé les premiers standards de cryptographie post-quantique (PQC). Trois algorithmes sont désormais standardisés :

| ALGORITHME | USAGE & CARACTÉRISTIQUES |
|---|---|
| Chiffrement<br>**ML-KEM (CRYSTALS-Kyber)** | Échange de clés et chiffrement. Algorithme de référence pour la protection des canaux de communication. Déjà adopté par Apple (iMessage), Google (Chrome) et Cloudflare. Sa faiblesse principale : si le problème M-LWE était résolu de manière inattendue, l'ensemble des systèmes basés sur Kyber tomberait simultanément — raison pour laquelle la diversité algorithmique est un impératif de robustesse systémique. |
| Signature<br>**ML-DSA (CRYSTALS-Dilithium)** | Signature numérique à haut débit. Recommandé pour l'authentification des communications gouvernementales et des transactions financières. Sa taille de signature est significativement plus grande que RSA ou ECDSA, ce qui impose une révision des hypothèses de bande passante dans certains protocoles (DNSSEC, passeports électroniques, certificats embarqués). |
| Signature<br>**SLH-DSA (SPHINCS+)** | Signature basée sur les fonctions de hachage. Plus lente mais considérée comme la plus robuste à long terme, sans hypothèse algébrique forte. Recommandée pour les cas d'usage à très longue durée de vie où la performance est secondaire — *firmwares* de systèmes critiques, archives nationales, racines PKI souveraines. L'ANSSI le recommande lorsque la durée de confiance dépasse 20 ans. |

En 2024, Apple[1] a déployé PQ3 dans iMessage — le niveau le plus élevé de sécurité cryptographique jamais déployé dans une messagerie grand public. Signal, WhatsApp et Cloudflare ont suivi. Le secteur privé technologique avance plus vite que la plupart des administrations publiques.

1. Apple Security, « iMessage with PQ3 » (security.apple.com) ; Apple Support, « Quantum secure cryptography in Apple operating systems ».

**Un quatrième standard, FALCON (FN-DSA),** est également finalisé pour les signatures nécessitant des petites empreintes. Il est plus compact que ML-DSA et convient aux environnements contraints (cartes à puce, IoT, SIM). Thales l'a utilisé dans ses travaux sur les SIM post-quantiques. Son implémentation est cependant plus délicate — les erreurs d'implémentation sur des cibles non sécurisées peuvent introduire des vulnérabilités par canaux auxiliaires (timing, consommation). Les certifications matérielles seront plus longues à obtenir.

L'Union européenne, via l'ENISA et l'ANSSI, a émis ses propres recommandations alignées sur ces standards, avec des adaptations pour les contextes souverains européens.

**La sélection d'HQC (*Hamming Quasi-Cyclic*) pour le quatrième round du concours KEM du NIST est un signal fort et un signe de vitalité européenne,** tandis que la normalisation officielle (FIPS 207) approche. HQC est fondé sur les codes correcteurs d'erreurs, une base mathématique radicalement différente des réseaux euclidiens. Sa sélection complémentaire à Kyber répond précisément à la logique de diversification des hypothèses mathématiques défendue par le CEA. La diversité algorithmique est en effet un élément clé de robustesse : « *Diversifier les bases mathématiques des algorithmes réduit le risque d'effondrement généralisé de la sécurité* » souligne le CEA. **Un portefeuille d'algorithmes dont les bases mathématiques sont indépendantes est plus robuste qu'un portefeuille homogène : la compromission d'une famille n'entraîne pas l'effondrement de l'autre.**

Pour les organisations qui déploient aujourd'hui, la recommandation pragmatique est d'implémenter ML-KEM + HQC en hybride là où les contraintes de performance le permettent. C'est une position de précaution renforcée que l'ANSSI soutient, et qui sera cohérente avec les futures recommandations du Quantum Act.

## II. La cryptographie hybride : la voie de transition pragmatique

En attendant la migration complète, la cryptographie hybride — combinant un algorithme classique (RSA, ECC) et un algorithme post-quantique — offre une protection immédiate. Si l'un des deux est compromis, l'autre maintient la sécurité. Cette approche est déjà recommandée par l'ANSSI, le BSI allemand et le NCSC britannique pour les systèmes sensibles.

**PQC vs QKD**

La PQC, fondée sur des hypothèses de complexité algorithmique, est déployable sur l'infrastructure réseau existante, sans matériel dédié, à des débits compatibles avec les usages actuels. Elle a donc gagné la bataille du déploiement de masse. Arnaud Dufournet, Directeur Marketing & Expérience Client TheGreenBow : *« la PQC s'est imposée comme la solution universelle. La QKD reste pertinente pour des cas d'usage souverains très spécifiques — liaisons diplomatiques point à point, datacenters gouvernementaux ultra-sensibles, réseaux militaires tactiques. »* Sa valeur n'est pas de remplacer la PQC mais de créer une couche souveraine inviolable pour les communications les plus critiques.

## III. La crypto-agilité : une approche de résilience

Elle consiste à être capable *« pour un système d'information de remplacer rapidement des algorithmes soudainement réputés faibles sans nécessiter de modifications majeures de l'architecture ou du code source d'un logiciel »* explique Arnaud Dufournet. Elle s'impose. *« Il faut démarrer le plus tôt possible la transition vers le post-quantique. L'intégration se veut longue et complexe. […] »* ajoute Ludovic Perret, professeur à l'EPITA.

L'ANSSI recommande une transition progressive et considère que des mécanismes hybrides combinant cryptographie classique et algorithmes post-quantiques peuvent constituer une approche pertinente.

CHAPITRE III

# ENJEUX SECTORIELS : CE QUI EST EN JEU

## 1. Défense et renseignement

- Les communications classifiées (réseaux gouvernementaux, liaisons diplomatiques, renseignement d'origine électronique) sont les cibles prioritaires de la stratégie HNDL.
- Les systèmes d'armes connectés et les plateformes C2/C4ISR ont des cycles de certification longs : la migration doit commencer immédiatement.
- L'interopérabilité OTAN impose une convergence des standards : les alliés qui tardent fragilisent l'ensemble de l'alliance

## 2. Secteur financier

- Les transactions SWIFT, les infrastructures de paiement, les registres blockchain et les systèmes de compensation sont fondés sur des algorithmes vulnérables.
- Un choc de confiance post-quantique — même partiel — sur les infrastructures financières pourrait déclencher une crise systémique.
- La Banque des Règlements Internationaux (BRI) et plusieurs banques centrales comme la Banque de France ont lancé de programmes d'évaluation PQC en 2024-2025.

## 3. Santé et données personnelles

- Les données médicales ont une valeur stratégique sur 50 à 70 ans (identité génétique, antécédents). Leur compromission future par HNDL est une menace grave pour les individus et les États.
- Les dispositifs médicaux connectés (pacemakers, pompes à insuline, imagerie) intègrent des protocoles cryptographiques souvent figés pour 15 à 20 ans.

## 4. Infrastructures critiques

- Les réseaux SCADA/ICS qui contrôlent l'énergie, l'eau et les transports utilisent des protocoles cryptographiques anciens souvent non mis à jour.
- La vulnérabilité quantique de ces réseaux est un vecteur potentiel de sabotage stratégique par des acteurs étatiques hostiles.

# LES ANGLES MORTS DE LA MIGRATION : CE QUE LES FEUILLES DE ROUTE NE DISENT PAS ASSEZ

## I. Le problème des systèmes *legacy* et des protocoles figés

L'immense majorité des analyses de migration PQC se concentre sur les nouvelles applications et les couches TLS. Mais le problème des systèmes embarqués, des protocoles industriels, des équipements réseau à longue durée de vie et des applications métier dont les cycles de certification imposent des contraintes drastiques est encore oublié.

Les systèmes SCADA/ICS qui contrôlent les réseaux d'énergie, d'eau et de transport embarquent souvent des implémentations cryptographiques compilées dans des *firmwares* figés pour 10 à 15 ans. Leur mise à jour nécessite des certifications réglementaires (IEC 62443, NERC CIP) dont les cycles sont de l'ordre de 2 à 5 ans. Pour ces systèmes, la fenêtre de migration est déjà sous tension. La bonne nouvelle industrielle vient de Thales : la démonstration d'une mise à jour OTA (Over-The-Air) des algorithmes cryptographiques sur SIM et eSIM sans remplacement physique ouvre une voie pour les équipements connectés. Le principe de crypto-agilité implémenté au niveau matériel — via des modules cryptographiques reconfigurables ou des HSM comme le *Datacryptor Model 5* — est la réponse architecturale correcte. Mais elle suppose que cette crypto-agilité ait été conçue dès l'origine dans l'équipement, ce qui n'est pas le cas de la majorité du parc installé.

> « *Un fabricant de puces intégrant aujourd'hui des composants cryptographiques dans des véhicules à conduite autonome conçoit des équipements qui seront en service dans 20 ans. Ces puces ne pourront pas être mises à jour. Si le RSA est compromis avant 2045, ces véhicules seront vulnérables. La question posée est claire : accepteriez-vous de conduire dans ce véhicule en sachant cela ? Ce n'est pas un cas d'école : c'est la réalité de l'industrie automobile, aéronautique et industrielle aujourd'hui.* »
>
> **Roberto De Paolis, Head of Digital Security & Security Operations, Leonardo.**

## II. PKI et identité numérique : le chantier le plus sous-estimé

L'ensemble des infrastructures à clé publique (PKI) — certificats TLS, identité numérique, horodatage, signature électronique — repose sur RSA et ECC et l'ensemble des applications qui en dépendent. La migration de ces infrastructures est un chantier titanesque qui conditionne la sécurité de l'ensemble du tissu numérique. La durée de vie des certificats racines est souvent de 20 à 30 ans. La migration doit être planifiée sur plusieurs années, avec des phases de coexistence où les deux infrastructures — classique et post-quantique — fonctionnent en parallèle.

Le projet RESQUE (consolidation des solutions VPN et HSM post-quantiques) financé par le Quantum Act européen s'attaque précisément à ce problème pour le périmètre gouvernemental européen. Mais la migration des PKI privées — secteur bancaire, santé, industrie — est largement sous-planifiée. La Banque de France et SWIFT ont démontré dans le projet LEAP que des transactions bancaires sécurisées par PQC sont techniquement opérationnelles. La feuille de route G7 (Cyber Expert Group) fixe 2030-2032 pour les systèmes critiques et 2035 pour l'ensemble des systèmes financiers. Ces délais sont techniquement tenables mais supposent que les travaux de migration PKI démarrent en 2026-2027 au plus tard.

## III. L'application métier : le nœud organisationnel, pas technique

> *« L'infrastructure PKI de Leonardo est désormais capable d'émettre des certificats avec des algorithmes* quantum-safe, *les HSM ont été mis à jour par firmware, et la plateforme d'orchestration est opérationnelle. Cette partie de la mise en place de l'infrastructure de sécurité est désormais terminée. Après deux ans de travail, l'infrastructure est prête. Ce qui reste — et c'est le plus difficile — c'est la couche applicative. Nous devons associer et convaincre les propriétaires d'applications et les responsables métier. C'est la partie la plus difficile du voyage, là où on touche le business. »*
> ***Roberto De Paolis, Head of Digital Security & Security Operations, Leonardo.***

Le problème n'est pas principalement technique. Il est organisationnel. Les propriétaires d'applications métier n'ont pas la conscience du risque cryptographique que portent leurs systèmes. Leur faire comprendre qu'ils ont un problème, puis les amener à planifier une mise à jour de leur application, requiert un travail d'évangélisation interne long et répétitif.

Une solution intermédiaire pour débloquer les situations où la mise à jour applicative n'est pas immédiatement possible est proposée : *« placer une couche de sécurité quantum-safe en amont de l'application, comme un "gilet de sauvetage" qui protège sans toucher au code, avec un délai fixé contractuellement pour la mise à jour définitive. Ce n'est pas une solution pérenne, mais c'est un compromis opérationnel qui permet de maintenir l'activité tout en avançant. L'alternative — attendre que l'application soit refondue avant de sécuriser — expose à une fenêtre de vulnérabilité inacceptable. »* témoigne Roberto De Paolis et d'ajouter : *« Lors d'une évaluation approfondie d'une application, la découverte que des bibliothèques comme OpenSSL sont utilisées dans des versions non à jour ralentit immédiatement la vitesse de migration. L'inventaire des dépendances des bibliothèques cryptographiques — pas seulement des algorithmes déclarés — est une étape que les équipes sous-estiment systématiquement. »*

## IV. Les middle-boxes : l'obstacle réseau invisible

Un angle mort propre aux infrastructures réseau mérite une attention particulière. Lors du passage d'une suite cryptographique classique TLS à un hybride post-quantique intégrant Kyber, la taille du premier message TLS passe de 32 octets à environ 1 216 octets. Cette augmentation de taille fait littéralement exploser de nombreux équipements de bordure — pare-feux, proxies, DPI, boîtiers d'inspection SSL — qui n'ont pas été conçus pour traiter des messages de cette taille. Les connexions sont coupées.

Ce problème, identifié empiriquement lors des expérimentations de Mozilla avec Cloudflare dès 2020-2022, a conduit à une stratégie délibérée : introduire de la variabilité systématique dans les protocoles (taille des messages, fréquence, fragmentation) pour forcer les constructeurs d'équipements réseau à mettre à jour leurs systèmes. En d'autres termes, "faire exploser les *middle-boxes*" est une étape intentionnelle de la transition, pas un effet secondaire indésirable.

Environ 25 à 26 % des connexions Internet sont aujourd'hui en hybride post-quantique ; avec Cloudflare seul, ce chiffre dépasse 50 %. Mais 20 % des connexions ne sont toujours pas à TLS 1.3, le standard de 2018 — ce qui illustre la durée réelle des transitions protocolaires à l'échelle d'Internet.

Pour les organisations gérant leurs propres équipements réseau, l'inventaire des middle-boxes et leur capacité à traiter des messages hybrides post-quantiques est une étape préliminaire indispensable à tout déploiement PQC sur les flux TLS.

CHAPITRE V

# DYNAMIQUE INTERNATIONALE : NE PAS RATER LE VIRAGE

## I. Une fragmentation qui pèse sur les entreprises

Les États-Unis ont émis en 2022 la *National Security Memorandum 10 (NSM-10)*, imposant aux agences fédérales un plan de migration PQC. La CISA coordonne la transition des infrastructures critiques. L'Union européenne a intégré la PQC dans sa stratégie de cybersécurité 2023-2028 et dans les révisions de la directive NIS2. L'OTAN a lancé en 2024 un groupe de travail dédié à l'interopérabilité post-quantique entre alliés. La Chine, de son côté, a lancé en 2025 un processus de standardisation PQC national (les SM-series étant des algorithmes classiques) et investit massivement dans l'informatique quantique.[2] Les capacités de collecte de renseignement électronique de grande puissance — NSA, GCHQ, FSB, MSS — sont présumées activer la stratégie HNDL depuis plusieurs années déjà.

Cette fragmentation crée un risque structurel pour les organisations internationales : une entreprise pharmaceutique ou aéronautique européenne avec des opérations en Chine, aux États-Unis et en Europe doit gérer trois référentiels cryptographiques distincts, potentiellement incompatibles à terme. Le coût de cette complexité est rarement intégré dans les estimations de migration PQC. De nombreux acteurs à dimension internationale font face à cette réalité : la migration PQC doit tenir compte des contraintes réglementaires de plusieurs juridictions simultanément.

Aussi, *« la coopération entre homologues européens est un impératif : la menace n'est pas nationale, et la fragmentation des approches affaiblirait la posture collective. Les échanges techniques portent notamment sur l'alignement des choix algorithmiques et des critères d'évaluation entre États membres, afin de garantir une transition coordonnée et sécurisée vers la cryptographie post-quantique (PQC). »* rappelle **Samih Souissi, Chef d'état-major Expertise, ANSSI.**

2. The Quantum Insider, « China Launches Its Own Quantum-Resistant Encryption Standards » (18 fév. 2025) ; The Quantum Insider, « China Expects Post-Quantum Cryptography Standards Within Three Years » (19 mars 2026).

## II. Le Quantum Act européen : enjeux et incertitudes

Le Quantum Act attendu pour 2027 est une étape décisive pour la souveraineté numérique européenne. Ses dispositions annoncées — obligation de migration PQC pour les infrastructures critiques d'ici 2028, interdiction des solutions non PQC dans les marchés publics à partir de 2030, financement de 3 milliards pour EuroQCI, PQC4eMRTD et RESQUE — constituent un signal fort. Mais plusieurs incertitudes méritent l'attention des décideurs. La date de 2028 pour les infrastructures critiques est ambitieuse. Pour les systèmes d'information gouvernementaux les plus complexes, deux ans de délai à partir de la publication du Quantum Act est très court. La réussite de ce calendrier suppose que les audits cryptographiques soient déjà en cours dans les administrations concernées — ce qui est loin d'être généralisé. Le Quantum Act est une étape clé pour notre indépendance technologique et *« l'opportunité est massive »* selon Constantijn van Oranje, membre du High-Level Advisory Board du Quantum Act,[3] *« mais elle exige une volonté de gagner »* rappelle-t-il souhaitant à la mise en oeuvre d'instruments de commande publique plus agiles et un renforcement significatif des fonds propres. Les organisations qui ne seront pas migrées vers la PQC d'ici 2030 seront, de facto, exclues des écosystèmes de confiance internationaux — marchés publics, coopérations industrielles, alliances de sécurité. La migration PQC est aussi un enjeu de souveraineté et de compétitivité.

3. déclarations lors d'un échange à Paris en janvier dernier dans le cadre d'un évènement organisé par Alice & Bob et le European Quantum Industry Consortium (QuIC).

## III. L'ANSSI, un rôle pivot

Le rôle de l'ANSSI dans la transition française est à la fois réglementaire (certification, qualification, recommandations) et stratégique (orientation de la R&D, animation de l'écosystème). Le signal de 2027 — la PQC sera indispensable pour obtenir des visas de sécurité — est un levier de marché considérable qui va accélérer les investissements des industriels. Or la qualification dure trois ans, et son processus d'instruction dépasse deux ans. Ce qui signifie, concrètement, que tout industriel souhaitant disposer d'un produit qualifié PQC disponible en 2030 doit avoir soumis un produit intégrant la PQC avant fin 2027. La fenêtre est donc étroite : les offreurs de solutions qui ne sont pas déjà en développement PQC actif aujourd'hui sont en retard.
Mais l'écosystème français n'a pas attendu. Bowrealis SecureTunnel de TheGreenBow, premier VPN client français intégrant les algorithmes PQC standardisés par le NIST, avec interopérabilité sur les passerelles souveraines (Thales Mistral, Eviden Trustway, Stormshield SN) et support de la RFC 9370, illustre la dynamique engagée.

L'ANSSI a également précisé sa vision pour les utilisateurs de solutions : la migration doit idéalement s'inscrire dans le cycle naturel de renouvellement des systèmes d'information. *« Si j'ai des marchés qui se terminent à telle date, je renouvelle avec mon fournisseur en version PQC. Si ce n'est pas disponible, je change de fournisseur. »* L'impératif est concret : dès aujourd'hui, toute DSI qui renouvelle un marché sans exiger une version PQC prend une décision stratégique par défaut dont les conséquences auront des répercussions significatives. Il est important de noter que pour les périmètres sensibles — Diffusion Restreinte notamment — intégrer la PQC dans les produit qualifié par l'ANSSI n'est pas une option mais une condition d'usage.
*« Ce n'est pas une recommandation vivement conseillée ; c'est une obligation. La distinction entre recommandation et obligation est ici fondamentale. »* ajoute Samih Souissi.

> « Les ministères, OIV et OSE consultés estiment avoir besoin de cinq ans pour déployer la PQC sur l'ensemble de leurs points de présence. En partant d'une arrivée d'un ordinateur quantique assez puissant pour mettre à mal la cryptographie entre 2035 et 2040, ce rétro-planning aboutit à 2030 comme date limite d'achat de produits non-PQC. Cette recommandation aura une portée normative en interministériel. *« À partir de 2030, aucun ministère ne devra plus acheter de produit cryptographique sans PQC. »*
> **Samih Souissi, Chef d'état-major Expertise, ANSSI.**

En parallèle, l'ANSSI développe également des POC d'accompagnement à destination des ministères et des OIV, avec l'ambition de définir des plans de transition reproductibles — reconnaissant que les contraintes organisationnelles et administratives sont souvent plus bloquantes que les contraintes techniques et accompagne les centres d'évaluation (les SST — Security Testing Labs) dans leur montée en compétences PQC, avec un objectif d'agrément à 2027 pour l'évaluation des produits intégrant de la PQC.
L'enjeu : disposer d'un corps d'évaluateurs compétents suffisant pour absorber la charge de certifications qui va s'accumuler.

> *« Aujourd'hui, les 10 CESTI (centres d'évaluation, hardware et software) doivent monter en compétence, conduire leurs projets pilotes et obtenir leur agrément PQC afin d'être capable d'évaluer des produits PQC d'ici 2027. »*
> **Samih Souissi, Chef d'état-major Expertise, ANSSI**

CHAPITRE VI

# LES DÉCISIONS STRATÉGIQUES QUE LES EXPERTS DOIVENT TRANCHER MAINTENANT

## I. Hybride ou natif PQC : la question du seuil de bascule

La recommandation de déployer des mécanismes hybrides (classique + PQC) dans la phase de transition est consensuelle. Mais la question du seuil de bascule vers le PQC natif — sans la composante classique — est moins souvent traitée. L'hybridation a un coût : *overhead* de calcul, complexité protocolaire, surface d'attaque élargie (deux algorithmes à maintenir). Pour les systèmes à forte contrainte de performance ou d'espace (IoT industriel, cartes à puce), ce coût peut être prohibitif.
La règle pratique émergente est la suivante : hybride pour les systèmes à longue durée de vie dont la migration complète sera échelonnée ; PQC natif dès la conception pour tout nouveau système dont le déploiement est postérieur à 2027. Pour les systèmes déjà déployés, l'hybridation est la voie de transition. Mais planifier dès aujourd'hui la date de sortie de l'hybridation — c'est-à-dire la bascule complète vers le PQC — est indispensable pour éviter que la période hybride ne devienne un état permanent par inertie organisationnelle.

## II. L'audit cryptographique : méthode et pièges

Un audit cryptographique rigoureux est plus difficile à conduire qu'il n'y paraît. Les inventaires déclaratifs — listes des algorithmes utilisés par les équipes — sont systématiquement incomplets. Les algorithmes cryptographiques sont présents dans des couches inattendues : bibliothèques de développement, *middlewares*, *firmwares* d'équipements réseau, protocoles d'authentification *legacy*, systèmes de gestion de certificats. La pratique recommandée est une approche combinant analyse statique du code (pour identifier les appels cryptographiques), analyse de trafic réseau (pour identifier les algorithmes négociés effectivement en production) et interrogation des fournisseurs sur leurs feuilles de route PQC.

*« La recommandation est d'exploiter les plateformes d'évaluation de vulnérabilités déjà déployées dans l'organisation pour extraire l'inventaire des certificats numériques utilisés — la plupart des organisations disposent déjà de ces outils sans les utiliser à cette fin. Il s'agit ensuite d'interroger les agents de protection des* endpoints *pour obtenir une cartographie des algorithmes utilisés au niveau serveur. Enfin, de déployer des capteurs réseau dans des segments spécifiques pour scanner et corréler l'ensemble. La synthèse de ces trois sources permet de construire un* "quantum risk score" *par application — une note de risque qui reflète la criticité des algorithmes utilisés (SHA-1 et MD5 en tête), permettant de prioriser les migrations par niveau de risque réel plutôt que par criticité nominale déclarée. »*
**Roberto De Paolis, Head of Digital Security & Security Operations, Leonardo.**

La notion de « durée de vie des données protégées » est le critère de priorisation le plus important et le plus souvent ignoré. Une donnée protégée par RSA-2048 dont la confidentialité n'a de valeur que 12 mois est une priorité faible. La même donnée dont la confidentialité doit tenir 15 ans est une priorité absolue. Cet axe — durée de vie des données plutôt que criticité nominale du système — doit structurer la feuille de route de migration.

## III. L'équation sécurité vs certification

À quel moment l'évaluation de sécurité opérationnelle doit-elle primer sur la certification formelle ? Préférez-vous être hors d'activité et certifié, ou en activité sans certification ? *« Pour les applications qui ne peuvent pas attendre le cycle complet de certification, déployer un protocole PQC expérimental — même non certifié — maintient le business opérationnel et crée une base d'expérience. L'important est de ne pas confondre l'absence de certification avec l'absence de niveau de sécurité. »* explique Roberto De Paolis. L'ANSSI nuance cette position sans la contredire : il y a un moment où le niveau de sécurité d'un algorithme n'est plus atteint, et à ce moment, la certification ne sert plus à rien — c'est le niveau de sécurité effectif qui compte. La mise à jour au bon moment doit primer. Une convergence de vue qui autorise les organisations à expérimenter sans attendre la certification complète, à condition que les périmètres les plus sensibles (Diffusion Restreinte notamment) restent sous le régime de qualification formelle.

## IV. La chaîne d'approvisionnement : le risque toujours invisible

La migration PQC d'une organisation ne vaut que ce que vaut la migration de ses fournisseurs critiques. Une organisation qui déploie ML-KEM sur ses propres serveurs mais dont le fournisseur de HSM, le prestataire de cloud ou l'éditeur de logiciel métier n'est pas migré maintient une surface d'attaque ouverte. Les clauses contractuelles PQC — exigence de feuille de route certifiée, délais de migration, droit d'audit — doivent être intégrées dans les renouvellements de contrats dès 2026. À partir de 2030, contracter avec le DoD américain sans PQC sera impossible : cette exigence va se diffuser rapidement dans les chaînes d'approvisionnement de la défense mondiale et, par extension, dans l'industrie duale.

# CE DONT LES EXPERTS DÉBATTENT ENCORE

## I. La robustesse à long terme de ML-KEM/ML-DSA

Malgré leur standardisation, les algorithmes fondés sur les réseaux euclidiens (Kyber, Dilithium) font l'objet d'une surveillance académique intense. Des résultats récents (2023-2024) ont montré que des variantes de l'attaque *two-step* peuvent, dans des configurations très spécifiques, affaiblir certaines implémentations. Ces attaques ne compromettent pas les paramètres standardisés, mais elles illustrent que la cryptanalyse post-quantique est un champ actif. La recommandation de conserver ML-KEM en hybride avec un algorithme à base mathématique différente (HQC ou SLH-DSA) n'est pas du conservatisme : c'est une réponse rationnelle à l'incertitude résiduelle. C'est la position que l'ANSSI défend explicitement.

## II. Les signatures PQC et le problème de la non-répudiation à long terme

La transition des signatures numériques soulève un problème juridique et technique rarement abordé : la non-répudiation à long terme. Une signature ECDSA apposée aujourd'hui sur un contrat de 20 ans sera-t-elle encore vérifiable et opposable en 2044, si ECDSA est compromis d'ici là ? La réponse technique passe par l'horodatage cryptographique renforcé (*timestamping*) et l'archivage des preuves de signature dans des formats post-quantiques. Les standards d'archivage à long terme (PAdES LTA, ETSI EN 319 142) sont en cours d'adaptation pour intégrer les signatures PQC. Pour les secteurs juridiques, notariaux, immobiliers et financiers où la force probante des signatures numériques est critique, ce chantier est urgent. Pour l'heure, ce qui est cependant actionnable dès aujourd'hui : travailler sur le processus de re-signature — qui déclenchera la re-signature, sur quels objets, selon quelle priorité — de sorte que, lorsque les standards seront prêts, le processus soit rodé et exécutable rapidement. La priorité n'est pas l'algorithme : c'est la gouvernance du processus de transition des signatures.

## III. La transition TLS à l'échelle d'Internet : un signal d'alarme sur les délais réels

La trajectoire de TLS 1.3 est un avertissement empirique que les décideurs doivent avoir intégré. Ce standard, finalisé en 2018 après quatre ans de travaux, est conçu nativement pour accueillir des primitives post-quantiques. En 2026, son taux d'adoption dans les navigateurs est de 80 %. Il reste donc 20 % des connexions qui ne sont toujours pas au standard de 2018 — après huit ans de déploiement. Sur les flux post-quantiques hybrides au sens strict, on est à 25-26 % à l'échelle d'Internet, et à plus de 50 % avec les partenaires les plus avancés. La leçon est simple : une transition protocolaire sur des systèmes à l'échelle d'Internet prend 10 à 15 ans pour atteindre une couverture quasi-complète. Quiconque pense pouvoir migrer l'ensemble de son SI en 2 à 3 ans n'a pas intégré cette réalité.

## IV. L’impact de l'IA sur la cryptanalyse post-quantique

Un angle émergent que les décideurs doivent commencer à intégrer : l'utilisation de l'intelligence artificielle pour accélérer la cryptanalyse, y compris des algorithmes post-quantiques. Des travaux récents explorent l'utilisation de réseaux de neurones pour résoudre des problèmes de type LWE dans des configurations spécifiques. Ces résultats sont préliminaires et ne menacent pas les paramètres standardisés actuels, mais ils introduisent une nouvelle variable dans l'équation de la durée de vie des algorithmes. La crypto-agilité prend ici tout son sens : une architecture capable de changer d'algorithme en quelques semaines sans refonte majeure est résiliente non seulement face à l'ordinateur quantique, mais aussi face à des percées cryptanalytiques inattendues d'origine classique ou hybride.

## V. La question des PME : le maillon faible de l’écosystème

La transition PQC est abordée sous l'angle des grandes organisations — armées, banques, OIV — qui disposent des ressources et des compétences pour l'entreprendre. Mais la chaîne de valeur industrielle intègre des PME sous-traitantes qui, elles, fournissent des composants, des logiciels ou des services à ces grandes organisations. Une PME qui fabrique des puces intégrées dans des systèmes industriels, ou qui développe un *middleware* utilisé dans une chaîne de paiement, est aussi concernée que l'OIV qui la mandate — et elle a moins de ressources pour agir. Pour ces acteurs, des solutions d'amorçage pragmatiques existent. La mise en place d'un VPN site-à-site avec des algorithmes symétriques — non vulnérables aux premières attaques quantiques — offre une protection immédiate sans refonte applicative. Des solutions "enveloppe de sécurité" placées en amont d'une application existante créent un canal *quantum-safe* sans toucher au code. Des outils d'auto-évaluation existent et permettent aux PME d'identifier les domaines prioritaires sans expertise préalable approfondie. Ces outils couvrent non seulement la dimension technologique mais aussi la gouvernance et la structure des équipes — car la crypto-agilité n'est pas qu'une question technique.

CHAPITRE VIII

# RECOMMANDATIONS STRATÉGIQUES POUR LES DÉCIDEURS

## 1. Inventorier avant de migrer : l'audit cryptographique

La première étape — et la plus urgente — est de dresser un inventaire exhaustif des actifs cryptographiques de l'organisation (*Cryptographic Asset Inventory*). Cela couvre : les algorithmes utilisés, les longueurs de clés, les protocoles déployés, les durées de conservation des données protégées, et les dépendances vis-à-vis de fournisseurs tiers. Sans cet inventaire, aucune stratégie de migration cohérente n'est possible.

## 2. Adopter la crypto-agilité comme doctrine

La crypto-agilité désigne la capacité d'un système à changer d'algorithme cryptographique sans refonte architecturale majeure. C'est la condition sine qua non pour une migration gérée dans la durée. Elle doit être intégrée dès la conception dans tout nouveau système d'information, tout nouveau contrat avec un fournisseur numérique, et toute révision d'infrastructure. Une feuille de route nationale est essentielle.

## 3. Déployer la cryptographie hybride à court terme

Dans l'attente de la migration complète, le déploiement d'algorithmes hybrides (classique + PQC) sur les communications les plus sensibles offre une protection immédiate contre la stratégie HNDL. Cette approche est techniquement disponible, standardisée et recommandée par les agences de cybersécurité françaises, européennes et américaines.

## 4. Former et gouverner

- Désigner un responsable de la transition post-quantique au niveau COMEX/CODIR, avec autorité transverse sur les directions SI, sécurité, juridique et achats.
- Intégrer les exigences PQC dans les clauses contractuelles avec les fournisseurs technologiques dès 2026.
- Former les équipes SI et sécurité aux algorithmes post-quantiques : la pénurie de compétences est déjà un facteur limitant.
- Participer aux exercices et groupes de travail sectoriels (ENISA, ANSSI, C5 Alliance) pour partager les retours d'expérience.

## 5. Planifier la migration sur 4 horizons

| | |
|---|---|
| **Immédiat (2026-2027)** | Audit cryptographique complet.<br>Déploiement hybride sur les flux les plus sensibles.<br>Crypto-agilité dans tous les nouveaux projets SI. |
| **Court terme (2028-2030)** | Assurer que tout produit entrant en processus de qualification ANSSI intègre bien la PQC hybride.<br>Migration des PKI et des systèmes d'authentification.<br>Mise à jour des systèmes embarqués et des équipements IoT.<br>Révision des contrats fournisseurs.<br>Commencer l'évangélisation des propriétaires d'applications métier |
| **Moyen terme (2030-2032)** | Migration complète des systèmes *legacy* et des équipements embarqués.<br>Sortir progressivement de l'hybridation sur les systèmes entièrement migrés en PQC natif.<br>Certification post-quantique des systèmes critiques.<br>Mise à jour des doctrines et des normes sectorielles. |
| **Long terme (2032-2035)** | Atteindre une posture PQC native sur l'ensemble du système d'information.<br>Réévaluer le portefeuille algorithmique en fonction des avancées de la cryptanalyse quantique et classique.<br>Contribuer à la consolidation des standards européens et internationaux via les retours d'expérience opérationnels. |

# L'URGENCE D'UNE DÉCISION

La cryptographie post-quantique n'est pas un sujet pour les équipes techniques : c'est un enjeu stratégique de premier rang qui appelle une décision au plus haut niveau de gouvernance. Les données sensibles collectées aujourd'hui contre lesquelles vous n'agissez pas sont potentiellement déjà compromises à terme.

La migration post-quantique est longue, complexe et coûteuse. La question n'est pas si la migration est nécessaire, mais si votre organisation sera en capacité de l'exécuter dans la fenêtre qui se ferme — et si les décisions pour y parvenir ont été prises au bon niveau de gouvernance, avec les ressources et l'autorité nécessaires.

Les organisations qui traiteront la migration PQC comme un projet technique délégué aux équipes SI échoueront. Celles qui en feront un programme stratégique piloté au plus haut niveau, intégrant les dimensions techniques, juridiques, contractuelles, opérationnelles et géopolitiques, construiront une résilience durable.

Le coût de l'inaction — compromission de données classifiées, rupture de confiance, exclusion des écosystèmes souverains, vulnérabilité opérationnelle — est structurellement plus élevé. Les organisations qui auront initié leur transition dès 2026 seront en position de force.
Celles qui attendront 2030 seront en situation de rattrapage d'urgence.

## RÉFÉRENCES & RESSOURCES CLÉS


- NIST FIPS 203, 204, 205 — Standards PQC (août 2024) : https://csrc.nist.gov/publications
- ANSSI — Guide de migration vers la cryptographie post-quantique (2024)
- ENISA — Post-Quantum Cryptography: Current state and quantum mitigation (2024)
- NSA/CISA — Cybersecurity Advisory on Post-Quantum Cryptography (2022–2025)
- ETSI Quantum Safe Cryptography Working Group — https://www.etsi.org/technologies/next-generation-technologies/
- TheGreenBow, Position Paper Crypto post-quantique : la transition s'accélère - https://www.thegreenbow.com/wp-content/uploads/2025/04/Note_de-Synthese_TGB_Crypto-Post-Quantique_La_transition_saccelere.pdf
- S&D Magazine - Cryptographie post-quantique et souveraineté : l'Europe à l'heure de la grande bascule - Mars 2026
- InCyber FORUM - Crypto-agility: Preparing for the Post-Quantum Transition - Avril 2026




Auteure : Mélanie BENARD-CROZAT
Conception graphique : ESPRIT COM'




Imprimé en France

## A propos de TheGreenBow

Créé en 1998, TheGreenBow est un éditeur français de logiciels de cybersécurité qui fournit des solutions d'accès distant sécurisé. Premier opérateur à avoir été certifié CC EAL3+, qualifié standard et agréé DR OTAN et UE en 2013, pour son logiciel Client VPN Windows, TheGreenBow s'impose comme la référence de l'accès distant de confiance et distribue ses logiciels dans plus de 70 pays. Depuis fin 2019, TheGreenBow détient le label « *Utilisé par les armées françaises* ». Ce label atteste de la confiance et de la mise en œuvre de ses technologies par les services du Ministère des Armées Françaises.

www.thegreenbow.com

THEGREENBOW