Menace Quantique sur RSA et AES : Guide DSI Complet

> Algorithme de Shor, harvest-now-decrypt-later, CRQC horizon 2030-2035 : ce que chaque DSI doit comprendre pour protéger son SI dès maintenant.

La menace quantique n'est plus une hypothèse de laboratoire réservée aux physiciens théoriciens. En 2026, les directions des systèmes d'information des grandes entreprises françaises font face à une réalité inédite : les algorithmes cryptographiques qui protègent leurs données depuis trente ans — RSA, ECC, Diffie-Hellman — seront mathématiquement vulnérables à des ordinateurs quantiques suffisamment puissants. Ce basculement ne s'opère pas du jour au lendemain, mais la fenêtre d'action se referme plus vite que la plupart des projets de transformation du SI. Comprendre précisément pourquoi RSA-2048 est condamné, pourquoi AES-256 résiste mieux, et surtout pourquoi vos adversaires collectent peut-être déjà vos flux chiffrés en anticipation du jour J, est désormais une responsabilité directe du DSI, au même titre que la conformité NIS 2 ou la gestion des vulnérabilités critiques.

Pourquoi les ordinateurs quantiques brisent RSA mais pas AES

Pour comprendre la menace, il faut distinguer deux catégories d'algorithmes cryptographiques selon leur fondement mathématique.

RSA, ECC et le problème de la factorisation

RSA repose sur la difficulté de factoriser un grand nombre en ses facteurs premiers. Multiplier deux nombres premiers de 1024 bits pour obtenir un nombre de 2048 bits est trivial. Faire l'inverse — retrouver les deux facteurs en connaissant uniquement le produit — est computationnellement infaisable pour un ordinateur classique. Les meilleurs algorithmes actuels de factorisation (General Number Field Sieve) nécessiteraient des millions d'années de calcul sur les supercalculateurs les plus puissants pour factoriser une clé RSA-2048.

L'algorithme de Shor, publié en 1994 par Peter Shor, change radicalement cette donne. Il démontre qu'un ordinateur quantique peut factoriser un entier N en temps polynomial — c'est-à-dire de façon exponentiellement plus rapide qu'un ordinateur classique. En pratique, un ordinateur quantique disposant d'environ 4000 qubits logiques stables pourrait casser RSA-2048 en quelques heures. La même logique s'applique à ECC (courbes elliptiques) via l'algorithme quantique de résolution du logarithme discret, et à Diffie-Hellman qui repose sur le même problème mathématique.

Ce sont donc toutes les infrastructures à clé publique — TLS, SSH, S/MIME, signatures numériques, PKI d'entreprise, VPN IPsec — qui sont directement menacées.

Pourquoi AES-256 résiste à la menace quantique

AES est un algorithme symétrique. Il ne repose pas sur la factorisation ou le logarithme discret, mais sur des opérations de substitution-permutation dans un espace mathématique différent. L'algorithme quantique de Grover peut accélérer la recherche exhaustive sur une clé symétrique, mais seulement d'un facteur racine carrée. Concrètement, AES-256 avec un ordinateur quantique offre une sécurité équivalente à AES-128 contre un attaquant classique — ce qui reste largement suffisant pour une protection à long terme.

La règle pratique pour les DSI : **le chiffrement symétrique (AES-256, ChaCha20) n'est pas en danger. Tout ce qui repose sur l'asymétrique (RSA, ECC, DH) doit être migré.**

À RETENIR

Points clés à retenir

L'algorithme de Shor permet à un ordinateur quantique de casser RSA et ECC en temps polynomial.

AES-256 reste sûr face aux ordinateurs quantiques (Grover réduit sa sécurité à l'équivalent d'AES-128, toujours suffisant).

TLS, SSH, PKI, VPN, signatures numériques — tout ce qui utilise de l'asymétrique est à risque.

L'horizon CRQC (Cryptographically Relevant Quantum Computer) est estimé entre 2030 et 2035 par les agences gouvernementales.

La menace harvest-now-decrypt-later est active dès aujourd'hui pour les données à longue durée de vie.

La timeline réaliste : quand un CRQC sera-t-il disponible ?

Un CRQC — Cryptographically Relevant Quantum Computer — est un ordinateur quantique capable de casser RSA-2048 en un temps raisonnable. Ce n'est pas l'ordinateur quantique actuel, qui reste limité à quelques centaines de qubits physiques bruités, loin des 4000 qubits logiques stables nécessaires.

> ⚡ **Retour terrain**
>
> Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

État des lieux en 2026

IBM a atteint 1127 qubits physiques avec son processeur Condor fin 2023. Google, avec Willow en décembre 2024, a démontré des qubits physiques avec des taux d'erreur inférieurs au seuil de correction quantique. Ces avancées sont significatives, mais la distance entre qubits physiques et qubits logiques reste considérable. Chaque qubit logique nécessite entre 1000 et 10 000 qubits physiques pour la correction d'erreurs, selon les architectures.

Les estimations des agences gouvernementales convergent vers un horizon 2030-2035 pour qu'un acteur étatique dispose d'un CRQC opérationnel. Certains experts comme Michele Mosca (Université de Waterloo) évaluent à environ 1/7 la probabilité qu'un CRQC casse RSA-2048 avant 2026 — probabilité qui monte à 50% avant 2031. Ces estimations varient, mais le consensus reste : nous ne sommes pas à cinq ans de l'évènement, mais nous n'en sommes probablement pas à vingt ans non plus.

Pourquoi 2030-2035 oblige à agir dès 2026

Les migrations cryptographiques à l'échelle d'un SI de grande entreprise prennent entre 5 et 10 ans. Les raisons sont multiples : inventaire de l'ensemble des usages cryptographiques (TLS interne, SSH, PKI, HSM, applications métier signées, workflows ETSI...), mise à jour des

bibliothèques et frameworks, recertification des systèmes critiques, négociation avec les éditeurs tiers, mise à jour des équipements réseau (VPN, firewalls), formation des équipes.

Si un CRQC opérationnel apparaît en 2032, les organisations qui commencent leur migration en 2028 arriveront trop tard. Celles qui commencent maintenant ont une chance de terminer à temps. C'est le message principal de l'ANSSI dans son document de recommandations sur la migration post-quantique, et c'est le même message porté par le NIST américain depuis la finalisation de ses standards en août 2024.

Harvest-Now-Decrypt-Later : la menace qui existe aujourd'hui

Il existe une catégorie de menace souvent sous-estimée par les DSI : le harvest-now-decrypt-later (HNDL). Le principe est simple et redoutable : un adversaire doté de capacités suffisantes — un État-nation en premier lieu, mais potentiellement des groupes criminels organisés disposant de ressources importantes — intercepte et stocke aujourd'hui des communications chiffrées avec les algorithmes actuels (RSA, ECC), dans l'attente de disposer d'un CRQC pour les déchiffrer dans 5 à 10 ans.

Qui pratique le HNDL et depuis quand ?

Les révélations Snowden de 2013 ont montré que la NSA collectait massivement du trafic chiffré. Il serait naïf de supposer que cette pratique a cessé, ou qu'elle est l'apanage des seuls États-Unis. La Chine, la Russie, et plusieurs autres États disposent de capacités d'interception massive. Les cibles prioritaires sont les communications diplomatiques, les transferts de propriété industrielle, les données de santé à valeur stratégique, les secrets commerciaux et les plans d'affaires.

Pour un DSI d'une entreprise française dans les secteurs de la défense, de l'énergie, de la santé, de la finance ou de l'industrie de pointe, la question n'est pas théorique. Si vos flux TLS contiennent aujourd'hui des informations qui auront encore de la valeur dans 10 ans — contrats à

long terme, données de R&D, plans industriels, données patients — ils constituent une cible HNDL crédible.

Les données à risque aujourd'hui

Le risque HNDL est proportionnel à deux facteurs : la sensibilité des données et leur durée de vie utile. Un tableau de bord de ventes hebdomadaire n'a aucune valeur dans 10 ans. En revanche :

Les données de R&D pharmaceutique ou industrielle gardent leur valeur 15 à 20 ans.

Les informations sur les infrastructures critiques (cartographie réseau, schémas SCADA) restent pertinentes des décennies.

Les données de santé individuelles sont protégeables pendant toute la vie de la personne.

Les secrets de négociation (M&A, contrats d'armement) peuvent rester sensibles 5 à 10 ans.

Les certificats racine et les clés de signature à longue durée de vie sont particulièrement exposés.

La politique de cryptographie conforme à l'ISO 27001 (A.8.24) doit désormais intégrer explicitement le risque HNDL dans l'analyse de risque, avec des durées de vie des clés adaptées et une classification des données par sensibilité quantique.

Algorithmes à risque : cartographie opérationnelle pour les DSI

Avant de planifier une migration, il faut comprendre où se cachent les algorithmes vulnérables dans un SI moderne.

TLS et HTTPS

TLS 1.2 et TLS 1.3 utilisent tous deux des algorithmes asymétriques pour l'échange de clés (ECDHE, DHE) et l'authentification des certificats (RSA, ECDSA). Même TLS 1.3, le plus récent, est vulnérable côté échange de clés. Les certificats de serveur (X.509) sont signés avec RSA ou ECC — deux algorithmes à migrer. TLS 1.3 avec Perfect Forward Secrecy (PFS) limite

le risque HNDL sur les sessions individuelles, mais ne protège pas les données applicatives si elles sont stockées après déchiffrement.

SSH

SSH utilise RSA, DSA, ECDSA ou Ed25519 pour l'authentification. Ed25519 (basé sur les courbes elliptiques) est également vulnérable à Shor. Les connexions SSH admin vers l'ensemble de votre infrastructure — serveurs, équipements réseau, systèmes industriels — sont donc exposées.

PKI d'entreprise

Les autorités de certification internes émettent des certificats RSA ou ECC. La CA racine, souvent avec une durée de vie de 20 ans, est un actif cryptographique critique. Sa compromission — même différée — invalide rétroactivement toutes les signatures émises. La migration PKI est généralement le chantier le plus complexe et le plus long.

VPN et IPsec

IKEv2, le protocole de négociation de clés d'IPsec, utilise Diffie-Hellman ou ECDH — deux algorithmes vulnérables. L'audit de sécurité de votre SI doit inclure un recensement exhaustif des tunnels VPN et de leurs suites cryptographiques.

Signatures de code et documents

Les signatures numériques appliquées aux documents (PDF, XML), aux mises à jour logicielles, aux contrats électroniques et aux workflows RH utilisent RSA ou ECC. Un document signé aujourd'hui avec RSA-2048 pourrait voir sa signature contestée en 2033 si son authenticité doit être prouvée devant un tribunal après la disponibilité d'un CRQC.

Messagerie et email

S/MIME et PGP, utilisés pour le chiffrement des emails sensibles, reposent intégralement sur RSA. Les emails chiffrés stockés dans les archives (conformité, archivage légal) constituent une cible HNDL de premier ordre pour les secteurs régulés.

Ce que vous devez faire concrètement en 2026

La réponse à la menace quantique n'est pas une réponse technologique ponctuelle. C'est un programme pluriannuel qui doit s'inscrire dans la gouvernance SSI de l'entreprise, aligné sur votre démarche ISO 27001 et votre stratégie de gestion des risques.

Phase 0 : Sensibilisation et gouvernance (maintenant)

Inscrivez la menace quantique dans votre analyse de risque SSI. Désignez un responsable du programme de migration post-quantique. Briefez votre COMEX sur le sujet — la décision de financer un programme pluriannuel de migration ne peut pas rester au niveau technique. Intégrez la cryptographie post-quantique dans vos critères d'achat pour les nouveaux systèmes (clause de crypto-agilité dans les cahiers des charges).

Phase 1 : Inventaire cryptographique (6-18 mois)

Il est impossible de migrer ce que vous ne connaissez pas. L'inventaire cryptographique consiste à identifier exhaustivement tous les usages d'algorithmes asymétriques dans votre SI : certificats TLS, clés SSH, configuration des VPN, bibliothèques cryptographiques embarquées dans les applications, workflows de signature, HSM et leur firmware. Des outils comme Keyfactor, Venafi Certificate Authority ou les scanners OpenSSL permettent d'automatiser partiellement cet inventaire.

Phase 2 : Priorisation par risque HNDL

Tous les systèmes n'ont pas la même urgence. Priorisez selon la sensibilité des données traitées et leur durée de vie. Les flux contenant des données à durée de vie supérieure à 5 ans doivent être traités en priorité. L'architecture Zero Trust peut aider à segmenter les flux sensibles et à cibler les efforts de migration.

Phase 3 : Migration par couches

La migration post-quantique s'effectue par couches, en commençant par les échanges de clés (hybridisation TLS + KYBER), puis les certificats (PKI hybride), enfin les signatures applicatives. Des solutions hybrides — qui combinent un algorithme classique et un algorithme post-quantique — permettent de maintenir la compatibilité avec les systèmes non encore migrés tout en ajoutant la protection post-quantique pour les connexions capables de l'utiliser.

La position de l'ANSSI et des référentiels français

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a publié en 2022 ses premières recommandations sur la cryptographie post-quantique, et les a complétées depuis. La position de l'agence est claire : les systèmes traitant des informations classifiées ou sensibles doivent amorcer leur migration immédiatement. Pour les systèmes non classifiés, l'agence recommande de commencer l'inventaire et la planification dès maintenant, et d'intégrer la crypto-agilité dans tout nouveau développement.

Le guide ANSSI sur la cryptographie post-quantique est la référence incontournable pour les DSI français. Il détaille les algorithmes recommandés, les stratégies de transition hybride et les priorités de migration selon les cas d'usage.

Dans le contexte de la politique cryptographique ISO 27001 (contrôle A.8.24), la migration post-quantique s'intègre naturellement comme une évolution de la politique de gestion des clés et des algorithmes approuvés. Les audits de certification ISO 27001 commencent à inclure des questions sur la posture post-quantique de l'organisation.

Risques réglementaires et contractuels

Au-delà du risque technique, les DSI doivent anticiper les implications réglementaires. Le RGPD impose de protéger les données personnelles avec un niveau de sécurité approprié à l'état de l'art. Si l'état de l'art en matière de cryptographie évolue vers le post-quantique (ce qui est déjà le cas dans les référentiels gouvernementaux), ne pas migrer pourrait être considéré comme un manquement aux obligations de l'article 32 du RGPD.

Les contrats avec des clients ou partenaires dans la défense, la santé ou les secteurs régulés incluent souvent des clauses sur les standards cryptographiques. Anticipez les demandes de vos clients qui vous demanderont, dans les prochaines années, des garanties sur votre conformité post-quantique. Ces exigences commencent à apparaître dans les appels d'offres publics des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) soumis à NIS 2.

Budget et ROI d'une migration post-quantique

La migration post-quantique est un investissement significatif, mais son coût doit être mis en regard du risque. Pour un SI de taille moyenne à grande (1000 à 10 000 utilisateurs), le coût d'une migration post-quantique complète — inventaire, outillage, licences, refactoring applicatif, formation — est typiquement de l'ordre de plusieurs centaines de milliers à quelques millions d'euros, étalé sur 5 à 7 ans.

Ce coût est à comparer au coût d'une violation de données massive dans un contexte post-CRQC : notification RGPD, amendes potentielles (jusqu'à 4% du CA mondial), atteinte à la réputation, pertes commerciales, responsabilité pénale des dirigeants. Sans parler du coût d'une migration effectuée dans l'urgence — généralement 3 à 5 fois plus cher qu'une migration planifiée.

Une approche progressive, intégrée aux cycles de renouvellement naturels du SI (renouvellement des certificats, upgrade des équipements réseau, refonte des applications), permet de lisser le coût et de minimiser les disruptions.

Interactions avec les projets SI en cours

La menace quantique n'est pas un projet isolé. Elle interagit avec plusieurs chantiers que vous avez probablement déjà en cours :

Zero Trust : L'architecture Zero Trust, en inventoriant et en microsegmentant les flux, crée la cartographie nécessaire à l'inventaire cryptographique post-quantique.

Cloud : Les migrations cloud impliquent souvent de renouveler les certificats et de reconfigurer les VPN — autant d'opportunités pour intégrer des suites post-quantiques dès maintenant.

PKI d'entreprise : Si votre CA racine arrive en fin de vie dans les 3 à 5 prochaines années, c'est le moment idéal pour passer à une PKI post-quantique ou hybride.

DevSecOps : Les pipelines CI/CD qui signent les artefacts logiciels doivent être adaptés pour utiliser des algorithmes post-quantiques. Intégrez cette exigence dans vos pipelines maintenant, avant que la prolifération des images et conteneurs à signer ne rende la migration plus complexe.

FAQ

Quel est l'horizon réaliste pour qu'un ordinateur quantique casse RSA-2048 ?

Les agences gouvernementales (NSA, ANSSI, ENISA) et la majorité des experts académiques s'accordent sur un horizon entre 2030 et 2035. Certains estiment que des acteurs étatiques bien dotés pourraient y parvenir dès 2028. Ces estimations sont incertaines par nature — une percée technologique imprévue pourrait accélérer ce calendrier. C'est pourquoi l'action doit commencer maintenant, indépendamment de la précision de ces prévisions.

AES-256 est-il vraiment sûr face aux ordinateurs quantiques ?

Oui, avec une nuance. L'algorithme de Grover permet à un ordinateur quantique de réduire la sécurité effective d'AES-256 à l'équivalent d'un AES-128 classique, soit 128 bits de sécurité. C'est toujours largement au-delà de ce qui est considéré comme sûr pour les décennies à venir.

En revanche, AES-128 utilisé seul tomberait à 64 bits de sécurité effective — insuffisant. Recommandation : utiliser AES-256 partout où c'est possible, dès maintenant.

Ma TPE ou PME est-elle concernée par la menace quantique ?

Les petites structures sont moins susceptibles d'être des cibles directes du HNDL étatique. Mais elles utilisent les mêmes protocoles TLS, SSH et PKI que les grandes entreprises. Lorsque les navigateurs et systèmes d'exploitation migreront vers les algorithmes post-quantiques (ce que Chrome, Firefox et Windows commencent déjà à déployer expérimentalement), les systèmes non compatibles rencontreront des problèmes de connectivité. La migration deviendra une nécessité opérationnelle, pas seulement sécuritaire.

Puis-je me contenter d'attendre que mes fournisseurs (Microsoft, Cisco, etc.) migrent à ma place ?

Partiellement. Microsoft, Cisco, AWS, Google Cloud et les principaux éditeurs intégreront progressivement le support post-quantique dans leurs produits. Mais la migration de la couche infrastructure ne couvre pas les certificats et clés propres à votre organisation, les applications métier développées en interne, les bibliothèques cryptographiques embarquées dans vos logiciels, ni les HSM (Hardware Security Modules) qui nécessitent souvent un remplacement matériel. Attendre uniquement vos fournisseurs serait insuffisant.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le

référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

