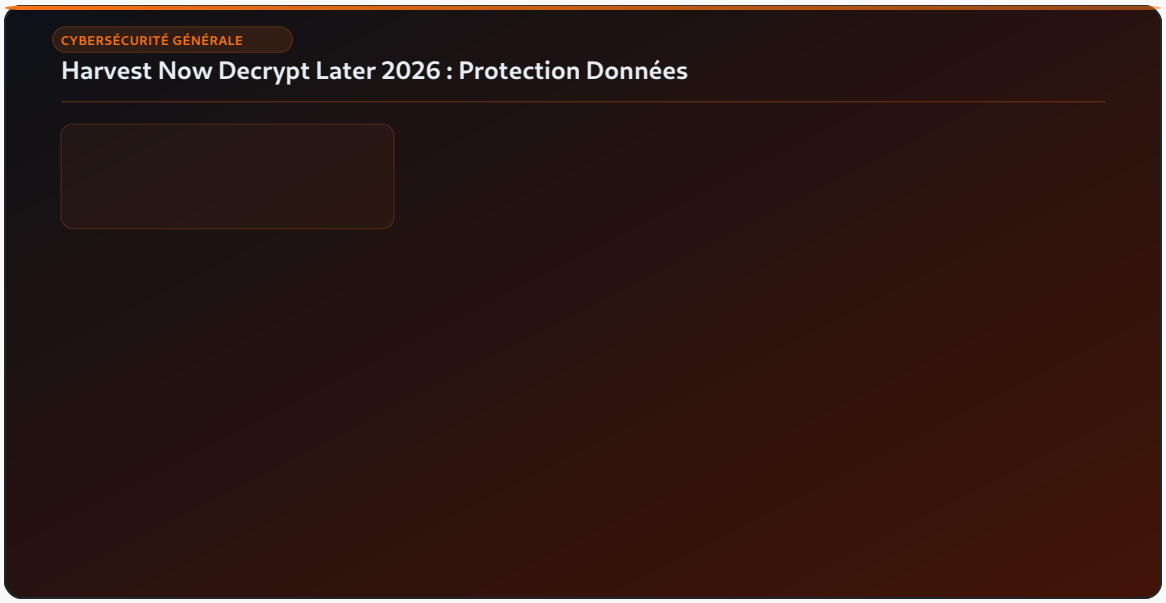
Harvest Now Decrypt Later 2026 : Protéger ses Données des Menaces Quantiques

> Comprendre la menace Harvest Now Decrypt Later et protéger ses données sensibles dès maintenant face à l'informatique quantique post-2030 — guide RSSI.

Imaginez un service de renseignement étatique qui intercepte depuis 2020 l'intégralité du trafic chiffré transitant par les câbles sous-marins reliant la France aux États-Unis. Ces données — emails confidentiels, transactions bancaires, communications gouvernementales, propriété intellectuelle industrielle — sont chiffrées avec RSA-2048 ou ECDSA. Aujourd'hui, elles sont illisibles. Mais dans dix à quinze ans, lorsqu'un ordinateur quantique suffisamment puissant sera disponible, il suffira de quelques heures pour déchiffrer rétroactivement ces archives. C'est précisément ce que décrit la menace **Harvest Now, Decrypt Later (HNDL)**, et c'est l'une des attaques les plus sophistiquées et les plus difficiles à contrer de l'histoire de la cybersécurité, parce qu'elle est passive, invisible, et que ses effets ne se manifestent qu'une décennie après sa mise en œuvre. Les agences de renseignement américaine (NSA), britannique (GCHQ) et française (DGSI/ANSSI) considèrent unanimement que des acteurs étatiques — notamment chinois et russes — pratiquent déjà cette collecte massive de données chiffrées en anticipation du Q-Day. Ce guide analyse les vecteurs d'exposition réels, les données à risque prioritaires, et les mesures de protection concrètes que les RSSI français doivent déployer dès maintenant pour réduire cette menace existentielle.

À RETENIR



HNDL est une attaque passive déjà active : des acteurs étatiques collectent du trafic chiffré depuis au moins 2015

Les données à durée de vie supérieure à 10 ans sont en danger immédiat — dossiers médicaux, IP industrielle, secrets d'État

Perfect Forward Secrecy (PFS) ne protège pas contre HNDL si l'adversaire capture le trafic réseau complet incluant les échanges de clés

La migration vers ML-KEM (TLS hybride) est la première défense déployable immédiatement

La classification et le rechiffrement des archives sensibles sont aussi urgents que la migration TLS

Anatomie de l'Attaque HNDL : Comment Elle Fonctionne

L'attaque Harvest Now, Decrypt Later repose sur une séquence en deux temps séparés par une fenêtre temporelle potentiellement décennale. Comprendre précisément cette mécanique est essentiel pour évaluer le risque réel et prioriser les actions défensives.

> ⚡ **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.

Temps 1 — La collecte (aujourd'hui) : l'attaquant capture et archive des volumes massifs de trafic réseau chiffré. Cette collecte peut s'opérer à plusieurs niveaux : interception sur les câbles sous-marins (level 1 infrastructure), compromission d'équipements réseau intermédiaires (routeurs BGP, équipements d'opérateurs), accès aux échanges de peering entre opérateurs, ou simplement collecte passive via des antennes directionnelles sur des liaisons microondes non filaires. La NSA pratique cette collecte à grande échelle depuis les révélations Snowden de 2013, et plusieurs analyses d'experts suggèrent que des programmes similaires existent en Chine sous le nom de code "Sea Cable".

Temps 2 — Le déchiffrement (futur) : une fois qu'un ordinateur quantique cryptographiquement pertinent (CRQC — Cryptographically Relevant Quantum Computer) sera disponible, l'attaquant exécutera l'algorithme de Shor pour factoriser les entiers RSA ou résoudre le logarithme discret ECDH des échanges de clés capturés. Cela lui permet de reconstituer les clés de session, puis de déchiffrer l'intégralité du trafic archivé. Le déchiffrement de plusieurs années d'archives pourrait prendre quelques jours sur un CRQC.

Le Q-Day : Quand l'Attaque Devient Réalité ?

La question du calendrier quantique est au cœur de toute stratégie de réponse HNDL. Sans horizon temporel, il est difficile de prioriser les investissements. Plusieurs estimations provenant de sources crédibles permettent de tracer un tableau raisonnable.

Le **rapport Mosca 2023** (Michele Mosca, Institut de l'informatique quantique de Waterloo) estime à 17% la probabilité qu'un CRQC capable de casser RSA-2048 existe avant 2031, et à 50% avant 2037. La plupart des experts en cryptographie quantique s'accordent sur une fenêtre de 2030-2040 pour l'avènement du premier CRQC opérationnel. IBM a annoncé son feuille de route vers un système quantique de 100 000 qubits logiques (nécessaire pour casser RSA-2048) pour 2033.

Ces estimations sont soumises à une forte incertitude dans les deux sens : des avancées technologiques imprévues pourraient accélérer l'échéance (comme la technique de correction d'erreurs "Magic State Distillation" optimisée par Google en 2024), ou au contraire des obstacles fondamentaux non encore découverts pourraient la repousser bien au-delà de 2040. La prudence stratégique impose de planifier pour le scénario pessimiste.

Source	Q-Day estimé	Probabilité avant 2030	Niveau de confiance
Mosca Institute 2023	2031-2037	17%	Élevé
NSA CNSA 2.0 (2022)	~2030 (implicite)	Non précisé	Élevé
ANSSI 2024	Horizon 2030-2035	Non précisé	Élevé
IBM Roadmap 2024	~2033 (technique)	Bas	Modéré

Classification des Données à Risque par Secteur

Toutes les données ne sont pas également exposées à la menace HNDL. Le niveau de risque dépend de deux facteurs : la **sensibilité intrinsèque** des données et leur **durée de vie requise de**

confidentialité. Un email de confirmation de livraison de 2024 sera sans intérêt en 2035 ; les plans de conception d'un réacteur nucléaire de 2024 seront encore hautement sensibles en 2050.

Dans le secteur **défense et aéronautique**, les données sont critiques : plans de conception d'armements, communications inter-alliés, technologies de furtivité. La durée de vie de confidentialité peut dépasser 30 ans. Ces organisations sont déjà soumises aux exigences ANSSI/DGA pour la migration PQC dans les systèmes qualifiés.

Dans le secteur **santé**, les dossiers médicaux électroniques ont une durée de conservation légale de 20 ans minimum (article R1112-7 du Code de la santé publique) et une valeur informationnelle très haute pour l'assurance, l'emploi, ou le chantage. Les hôpitaux et mutuelles sont des cibles HNDL prioritaires.

Dans le secteur **industriel et R&D**, les brevets en instance, les formules chimiques, les algorithmes propriétaires représentent une valeur stratégique sur 10 à 20 ans. La France a été victime de plusieurs campagnes d'espionnage industriel étatique documentées par l'ANSSI et la DGSI.

Données prioritaires à protéger contre HNDL

Santé : dossiers patients, résultats génétiques, données psychiatriques

Défense : communications classifiées, plans techniques, renseignement

Finance : transactions long terme, données de credit scoring, archives AML

R&D industrielle : brevets, formules, algorithmes propriétaires

Juridique : communications avocat-client, accords de fusion-acquisition

Énergie/OT : plans d'infrastructure critique, protocoles de sécurité ICS

Pourquoi Perfect Forward Secrecy Ne Suffit Pas

Un mythe répandu en sécurité affirme que Perfect Forward Secrecy (PFS) protège contre HNDL. C'est une simplification dangereuse qu'il faut déconstruire précisément, car elle peut conduire des RSSI à différer la migration PQC en se croyant faussement protégés.

PFS classique (ECDHE) : Dans un échange TLS avec PFS, le serveur génère une paire de clés éphémère (ECDH) pour chaque session. La clé privée de cette paire éphémère est détruite après la session. Si la clé privée du certificat serveur est compromise, elle ne permet pas de déchiffrer les sessions passées — c'est la propriété que PFS garantit.

La vulnérabilité HNDL avec PFS : Cependant, si un adversaire capture le trafic réseau complet — y compris les paquets ClientHello et ServerHello contenant l'échange de clés ECDHE — il peut, avec un ordinateur quantique, résoudre le problème du logarithme discret sur la courbe elliptique ECDHE et retrouver la clé de session. PFS protège contre la compromission de la clé serveur à long terme, mais pas contre un adversaire qui stocke l'échange de clés ECDHE lui-même. Et c'est précisément ce que font les programmes de surveillance massive : ils capturent le trafic brut complet, pas seulement les données applicatives.

La conclusion est sans appel : **PFS avec algorithmes classiques (ECDHE) ne protège pas contre HNDL**. Seule l'hybridisation avec ML-KEM (qui résiste aux attaques quantiques sur l'échange de clés) offre une protection réelle.

Inventaire des Archives Sensibles : Une Priorité Souvent Oubliée

La migration TLS vers des algorithmes post-quantiques protège les communications futures — mais qu'en est-il des données chiffrées stockées dans vos archives ? Des emails chiffrés en S/MIME depuis 2015, des fichiers chiffrés avec RSA stockés dans votre DMS, des sauvegardes chiffrées avec des clés RSA-2048 en dormance dans vos tapes — tout cela reste vulnérable à une attaque HNDL si votre adversaire dispose déjà d'une copie de ces données.

L'inventaire des archives sensibles doit identifier : les **emails archivés chiffrés en S/MIME** (Exchange, Lotus Notes archives), les **fichiers chiffrés avec des solutions PGP, VeraCrypt ou**

BitLocker (pour BitLocker, la clé de chiffrement de volume est protégée par le TPM + PIN, sans chiffrement asymétrique exposé — risque moindre), les **communications enregistrées dans des systèmes de collaboration** (Slack, Teams, archives vidéo de visioconférences).

Menaces HNDL Documentées : Ce que Disent les Services de Renseignement

La menace HNDL n'est pas une spéculation académique : elle est explicitement documentée par plusieurs services de renseignement occidentaux dans leurs communications publiques. Analyser ces sources officielles permet de calibrer l'urgence réelle de la réponse.

La **NSA (National Security Agency)** américaine a publié en septembre 2022 ses directives CNSA 2.0 (Commercial National Security Algorithm Suite 2.0), qui imposent la migration vers les algorithmes post-quantiques pour tous les systèmes de sécurité nationale avant 2033. Cette échéance non négociable, fixée par la plus grande agence de cybersécurité au monde, est un signal fort. La NSA a motivé cette décision par la nécessité de protéger les systèmes contre des adversaires qui "collectent dès maintenant des données chiffrées en anticipation des capacités cryptanalytiques futures".

Le **GCHQ britannique**, via son bras opérationnel le NCSC, a publié en 2024 une guidance similaire pour les organisations UK Critical National Infrastructure, avec une mention explicite de la menace HNDL et des pratiques de collecte passive attribuées à des acteurs étatiques chinois et russes. Le NCSC recommande une migration vers les algorithmes post-quantiques avant 2028 pour les systèmes protégeant des données à longue durée de vie.

La **DGSI** (Direction Générale de la Sécurité Intérieure) française a produit en 2023 une note de sensibilisation non publique sur les risques d'espionnage économique quantique, distribuée aux entreprises stratégiques françaises via le réseau des correspondants régionaux. Cette note mentionne des activités documentées de collecte de données chiffrées par des services de renseignement étrangers ciblant spécifiquement les données de R&D française dans les secteurs de l'aéronautique, du nucléaire et de la pharmaceutique.

Évaluation de Maturité Anti-HNDL : Grille d'Autoévaluation

Pour permettre à chaque organisation d'évaluer rapidement sa maturité face à la menace HNDL, voici une grille d'autoévaluation en 10 questions. Répondez par Oui (1 point) ou Non (0 point) à chaque question.

Question	Score Oui
Avez-vous un inventaire des données à durée de vie >10 ans ?	1
Vos frontaux TLS utilisent-ils l'hybridisation ML-KEM ?	1
Vos archives sensibles sont-elles chiffrées avec AES-256 ?	1
Avez-vous une feuille de route PQC validée par la direction ?	1
Vos VPN IPsec utilisent-ils PFS avec ECDHE ou DHE ?	1
Avez-vous un inventaire cryptographique complet de votre infrastructure ?	1
Vos HSM ont-ils une roadmap PQC fournisseur confirmée ?	1
HNDL figure-t-il dans votre registre des risques cyber ?	1
Vos équipes ont-elles été formées aux bases de la PQC ?	1
Avez-vous un budget alloué pour la migration PQC 2025-2030 ?	1

Score 0-2 : exposition critique — aucune défense HNDL en place. Score 3-5 : exposition élevée — quelques mesures isolées sans cohérence stratégique. Score 6-8 : exposition modérée — programme PQC en cours, axes d'amélioration identifiés. Score 9-10 : exposition faible — maturité PQC avancée, programme en bonne voie.

Approche Zero Trust et HNDL : Réduire la Surface d'Interception

L'architecture Zero Trust, bien que conçue pour un autre type de menace (l'attaquant déjà dans le réseau), contribue indirectement à réduire la surface d'exposition HNDL. En segmentant le trafic réseau, en chiffrant les communications internes (east-west), et en réduisant la durée de vie des sessions, Zero Trust diminue le volume de données qu'un adversaire peut collecter en une seule session d'interception.

mTLS systématique dans une architecture Zero Trust (entre microservices, entre segments réseau) signifie que même un adversaire ayant compromis un point d'interception interne ne peut pas déchiffrer les communications entre services. La combinaison Zero Trust + hybridisation TLS post-quantique offre une défense en profondeur particulièrement robuste contre HNDL.

Pour les équipes DevOps qui implémentent Zero Trust via des service meshes (Istio, Linkerd, Consul Connect), la migration vers des algorithmes PQC peut être réalisée de façon centralisée dans la configuration du mesh — sans modification du code applicatif. C'est l'un des bénéfices architecturaux majeurs de Zero Trust dans le contexte PQC.

Stratégie de Rechiffrement des Archives Critiques

Pour les données les plus sensibles avec une exposition HNDL avérée, la stratégie de rechiffrement consiste à déchiffrer les données avec les clés classiques actuelles, puis à les rechiffrer avec AES-256-GCM (qui est post-quantique résistant nativement) sous une nouvelle clé protégée par ML-KEM.

```
 # Exemple de script de rechiffrement d'archives email S/MIME
# Étape 1 : Déchiffrement avec la clé RSA actuelle
openssl smime -decrypt -in archive_2020.eml \
  -inkey private_key_rsa2048.pem \
  -out decrypted_content.txt

# Étape 2 : Rechiffrement avec AES-256-GCM symétrique
# (clé AES elle-même protégée par ML-KEM via envelope)
openssl enc -aes-256-gcm -pbkdf2 -iter 600000 \
  -in decrypted_content.txt \
  -out archive_2020_pqc.enc

# Supprimer les données déchiffrées intermédiaires
shred -vuz decrypted_content.txt
```

Solutions HSM Post-Quantiques pour la Protection à Long Terme

Les HSM (Hardware Security Modules) jouent un rôle central dans la défense contre HNDL pour les données les plus sensibles. En 2026, plusieurs fournisseurs proposent des HSM avec support post-quantique en production ou en preview.

Thales Luna HSM (firmware 7.8+) supporte ML-KEM-512/768/1024 et ML-DSA-44/65/87 via un module logiciel. Le support matériel natif (accélération crypto PQC dans le processeur HSM) est annoncé pour les modèles Luna Network 7 generation 2 en 2026. **Utimaco SecurityServer Se Gen 2** offre un support expérimental ML-KEM depuis le firmware 5.0. **AWS CloudHSM** a annoncé le support de ML-KEM et ML-DSA pour le premier semestre 2026, et Azure Dedicated HSM suit un calendrier similaire.

Pour les organisations ne pouvant pas encore migrer leurs HSM physiques, une approche intermédiaire consiste à utiliser un **software HSM post-quantique** (SoftHSM 2.6+ avec liboqs) pour les opérations non critiques, en attendant le support matériel. Cette approche offre les algorithmes PQC mais sans les garanties de sécurité physique d'un vrai HSM.

Migration TLS : Déploiement Pratique de l'Hybride ML-KEM

La première ligne de défense contre HNDL pour les communications futures est l'activation de l'hybridisation ML-KEM sur tous les terminaisons TLS. Voici les étapes pratiques pour les environnements les plus courants en entreprise française.

Pour **Nginx** : mettre à jour vers OpenSSL 3.4+ avec le provider OQS, puis configurer les groupes hybrides dans ssl_ecdh_curve. Pour **Apache** : même prérequis OpenSSL, configuration dans SSLOpenSSLConfCmd Curves. Pour **Java/Spring Boot** : JDK 21+ avec Bouncy Castle 1.78+ fournit ML-KEM dans l'API Java Security Standard. Pour **Go** : le package `golang.org/x/crypto/mlkem` est disponible depuis Go 1.23 (expérimental), avec une API stable prévue pour Go 1.25.

Surveillance et Détection : Identifier les Activités de Collecte HNDL

Bien que HNDL soit une attaque passive difficile à détecter, certains indicateurs peuvent signaler des activités suspectes de collecte réseau dans votre environnement ou à proximité.

Les **équipements réseau compromis** (routeurs, switches, pare-feux) constituent le premier vecteur de collecte. Une surveillance des configurations réseau via des outils comme Cisco CiscoWorks, SolarWinds NCM ou Zabbix peut détecter des modifications non autorisées de configurations d'export de trafic (SPAN, RSPAN, ERSPAN, Netflow vers des destinations non reconnues).

Les **anomalies de peering BGP** sont un autre indicateur. Des détournements BGP (BGP hijacking) permettent de router temporairement du trafic via des réseaux contrôlés par l'attaquant. Des services comme BGPMon ou RIPE NCC BGP Hijack Detection peuvent alerter sur des routes suspectes pour vos préfixes IP.

Anecdote terrain : la collecte via l'opérateur

En 2024, lors d'un audit de sécurité dans un groupe pharmaceutique français, nos équipes ont découvert que le routeur de bordure était configuré avec un export Netflow non documenté vers une adresse IP appartenant à un opérateur télécoms étranger. La configuration datait de 2019 et n'avait pas été détectée lors des audits précédents car elle était présente dans une section du fichier de configuration rarement inspectée. L'export incluait uniquement les métadonnées (IP source/destination, ports, volumes) — pas le contenu — mais pour une entreprise dont l'essentiel du business passe par des VPN vers des partenaires industriels, ce type de collecte de métadonnées suffit à reconstituer le schéma d'activité. Un point de collecte HNDL dormant depuis 5 ans, potentiellement.

HNDL dans le Contexte des Communications Gouvernementales et OIV

Les organismes publics et les Opérateurs d'Importance Vitale (OIV) sont des cibles prioritaires des programmes HNDL étatiques. La nature même de leurs données (décisions gouvernementales, plans d'infrastructure critique, stratégies défensives nationales) justifie une attention particulière des services de renseignement adverses avec des horizons de déclassification de 10 à 30 ans.

L'ANSSI a développé et qualifié des solutions de communication sécurisée PQC pour les ministères et OIV, notamment via le programme **Cryptowall** et les produits Pastis et Mistral qui intègrent des mécanismes post-quantiques. Pour les entités hors périmètre ANSSI, des solutions commerciales qualifiées comme les VPN **Stormshield SN** avec firmware PQC ou les boîtiers **Cisco Quantum-Safe** sont disponibles.

Analyse des Vecteurs de Collecte : Comment les Données sont Interceptées

Comprendre les vecteurs techniques par lesquels des acteurs malveillants collectent des données pour des attaques HNDL permet d'identifier les zones d'exposition prioritaires et d'y concentrer les efforts défensifs. Les vecteurs de collecte se répartissent en quatre catégories selon leur niveau d'infrastructure.

Niveau 1 — Infrastructure physique : l'interception sur les câbles sous-marins est le vecteur le plus massif mais aussi le plus difficile à contrer au niveau organisationnel. Les grandes puissances disposent de sous-marins espions capables de connecter des dispositifs d'écoute sur les câbles en fibres optiques sous-marins à grande profondeur. Les données transitant entre continents sur ces câbles sont capturées, copiées et archivées. Cette technique, connue sous le nom de "Cable Tap", nécessite des moyens étatiques importants mais permet d'intercepter plusieurs térabits de données par seconde.

Niveau 2 — Points d'échange Internet (IXP) : les Internet Exchange Points comme France-IX (Paris), DECIX (Francfort) ou AMS-IX (Amsterdam) concentrent des volumes énormes de trafic Internet. Une compromission d'équipements dans ces nœuds, ou un accès légal forcé via des procédures de surveillance légale, permet d'accéder à des volumes massifs de trafic. Les nœuds IXP sont des cibles de haute valeur pour les services de renseignement.

Niveau 3 — Opérateurs télécoms : les opérateurs Internet (Tier 1 et Tier 2) transportent l'intégralité du trafic de leurs clients. Des accès légaux forcés (via des procédures d'interception légale comme les IMSI catchers ou les équivalents pour les communications IP), des compromissions d'équipements réseau, ou des partenariats forcés par des régimes autoritaires permettent la collecte ciblée ou massive de trafic client.

Niveau 4 — Équipements réseau d'entreprise compromis : des campagnes d'APT (Advanced Persistent Threats) ciblent spécifiquement les équipements réseau d'entreprise (routeurs Cisco, pare-feux Palo Alto, VPN Fortinet) pour y installer des implants qui exportent silencieusement une copie du trafic vers des serveurs contrôlés par l'attaquant. L'alerte ANSSI de janvier 2024 sur les attaques APT31 ciblant des équipements Cisco en France illustre ce vecteur.

Protection des Données au Repos : Chiffrement à Longue Durée de Vie

En parallèle de la protection des communications (TLS hybride), la protection des données stockées au repos est le second pilier de la défense HNDL. Les données sensibles stockées sur vos systèmes — bases de données, sauvegardes, archives documentaires — doivent être chiffrées avec des algorithmes résistants aux attaques quantiques.

La bonne nouvelle : **AES-256 est déjà post-quantique résistant**. Si vos données au repos sont chiffrées avec AES-256 (BitLocker avec chiffrement complet, dm-crypt sous Linux, chiffrement de base de données transparente Oracle TDE ou SQL Server TDE en mode AES-256), vous êtes protégés contre les attaques quantiques sur le payload. Le risque résiduel concerne uniquement les mécanismes de gestion des clés : si la clé AES-256 est elle-même protégée par RSA ou ECDSA (comme dans de nombreuses architectures d'enveloppe de clé), cette couche externe est vulnérable.

La priorité est donc de **migrer les systèmes de gestion de clés (KMS)** vers des mécanismes post-quantiques. AWS KMS, Azure Key Vault et HashiCorp Vault ont des roadmaps pour intégrer ML-KEM dans leurs mécanismes d'enveloppe de clé. Pour les KMS on-premise, la migration nécessite une coordination avec les fournisseurs HSM.

Géopolitique de HNDL : Acteurs, Programmes et Cibles Prioritaires

Comprendre qui conduit des programmes HNDL et quelles sont leurs cibles prioritaires aide les organisations françaises à évaluer leur propre niveau de risque. Si votre organisation n'est pas une cible pertinente pour les services de renseignement étrangers, le risque HNDL — bien que non nul — est significativement plus faible que pour une entreprise du CAC 40 ou un opérateur d'importance vitale. Cette calibration permet d'allouer les ressources défensives de façon proportionnée.

Les **programmes étatiques de collecte massive** documentés ou fortement suspectés incluent : le programme PRISM (NSA, USA) ciblant les principales plateformes Internet ; le programme

Tempora (GCHQ, UK) de collecte sur les câbles sous-marins transitant par le Royaume-Uni ; les opérations chinoises attribuées aux groupes APT40 et APT10 ciblant la propriété intellectuelle dans les secteurs de la défense, de l'aéronautique et de la pharmacie ; et les opérations russes (APT28/Fancy Bear, APT29/Cozy Bear) ciblant les institutions gouvernementales et les think tanks occidentaux. La France, qui héberge de nombreuses entreprises stratégiques dans ces secteurs, est une cible prioritaire de plusieurs de ces programmes.

Les **cibles de valeur prioritaire** pour une collecte HNDL par des acteurs étatiques sont typiquement : les contrats d'armement et les spécifications techniques associées (secteur défense), les projets nucléaires civils et militaires (EDF, CEA, ORANO), les travaux de R&D en pharmacologie et en biotechnologie (Sanofi, Institut Pasteur), les stratégies de fusion-acquisition des grands groupes français, et les communications diplomatiques entre institutions françaises et partenaires européens ou alliés.

Contractualisation PQC avec les Fournisseurs et Sous-Traitants

Un aspect souvent négligé de la stratégie anti-HNDL est la chaîne de sous-traitance. Si vos communications internes sont protégées par des algorithmes post-quantiques mais que vos échanges avec des fournisseurs critiques (intégrateurs, prestataires cloud, partenaires EDI) utilisent des algorithmes classiques, la menace HNDL reste présente sur ces flux externalisés. La mise à jour des contrats et SLA avec les fournisseurs est un levier contractuel souvent sous-exploité.

Les organisations matures en cybersécurité commencent à inclure des **clauses de maturité cryptographique post-quantique** dans leurs contrats IT. Ces clauses typiquement exigent que le fournisseur dispose d'un inventaire cryptographique à jour, publie sa feuille de route PQC, et s'engage à migrer vers des algorithmes hybrides sur les connexions avec le client avant une date définie (généralement 2027-2028). Des audits annuels de conformité PQC peuvent être intégrés dans les plans d'audit fournisseurs.

Cette approche est particulièrement pertinente pour les **éditeurs de logiciels métier** (ERP, CRM, SIRH) dont les API intègrent souvent des mécanismes cryptographiques propres (tokens d'authentification, chiffrement de données en transit entre modules). Exiger de votre éditeur SAP,

Salesforce ou Workday une roadmap PQC documentée pour leurs API est une démarche parfaitement légitime que les services achats doivent intégrer dans leurs critères d'évaluation.

Outils de Simulation et de Test Anti-HNDL

Plusieurs outils permettent aux équipes sécurité de tester et de valider leur posture défensive contre HNDL, en simulant des scénarios d'interception et en vérifiant que les mécanismes post-quantiques sont correctement déployés.

OQS-TLS-Demo (Open Quantum Safe Project) est un environnement de test complet incluant un serveur et un client TLS supportant tous les algorithmes NIST PQC en mode hybride. Il permet de vérifier que vos équipements réseau (WAF, load balancer, proxy) ne bloquent pas les échanges de clés hybrides, et de mesurer l'impact performance sur votre infrastructure spécifique.

Wireshark avec dissecteurs OQS permet d'analyser des captures de trafic TLS hybride et de vérifier que les extensions Kyber sont bien présentes dans les handshakes. Un audit régulier des captures de trafic TLS peut confirmer que l'hybridisation est bien active sur tous les endpoints cibles et non uniquement sur ceux testés lors du déploiement initial.

testssl.sh en version 3.1+ supporte la vérification des suites cipher post-quantiques hybrides. Intégré dans un pipeline de tests de sécurité automatisé (CI/CD ou scanner périodique), il garantit que les frontaux TLS restent conformes après chaque mise à jour de configuration ou de certificat.

Chiffrement de Bout en Bout et HNDL : Applications de Messagerie

Les applications de messagerie chiffrée de bout en bout (Signal, WhatsApp, Telegram Secret Chats, ProtonMail) offrent une couche de protection supplémentaire contre HNDL par rapport au simple TLS. Avec E2EE, même si un adversaire capture le trafic au niveau de l'opérateur télécom

ou du serveur, il ne peut pas déchiffrer le contenu des messages sans avoir accès aux clés privées des appareils terminaux.

Cependant, ces applications utilisent actuellement des algorithmes classiques (Signal Protocol utilise X3DH basé sur ECDH, et Double Ratchet avec Curve25519). Face à HNDL, elles sont donc vulnérables si l'adversaire capture le trafic chiffré des sessions passées. **Signal** a annoncé en 2023 la migration de son protocole d'établissement de clés vers PQXDH (Post-Quantum Extended Diffie-Hellman), intégrant Kyber-1024 en hybride avec ECDH X25519 — une avancée majeure qui protège les nouvelles sessions Signal contre HNDL. Cette migration a été déployée dans Signal 6.43+ sur iOS et Android.

Pour les communications d'entreprise, l'utilisation de solutions E2EE migrant vers PQC est à privilegier pour les échanges les plus sensibles. Des solutions comme **Olvid** (messagerie française certifiée ANSSI) ont une roadmap PQC publique. La recommandation de l'ANSSI pour les communications sensibles est d'utiliser uniquement des solutions dont la roadmap PQC est connue et publiée.

Synthèse : Matrice de Priorité Anti-HNDL par Criticalité

Pour aider les RSSI à prioriser leurs actions anti-HNDL dans un contexte de ressources limitées, voici une matrice de priorité croisant la valeur des données avec leur durée de vie. Cette matrice définit l'ordre de traitement recommandé pour une organisation de taille moyenne (100 à 2000 employés) sans programme PQC préexistant.

Les actions de priorité absolue sont : (1) activer l'hybridisation TLS ML-KEM sur tous les accès Internet — 1 à 2 semaines, impact maximal pour un effort minimal ; (2) identifier et isoler les archives d'emails chiffrés avec S/MIME datant de plus de 5 ans — risque HNDL passé non couvrable mais à quantifier ; (3) vérifier que toutes les données sensibles au repos sont chiffrées avec AES-256 et non AES-128 ou DES (encore présent dans de nombreux systèmes legacy).

Les actions de priorité haute à planifier dans les 6 prochains mois : audit des HSM et de leur roadmap PQC fournisseur, migration des connexions VPN site-à-site vers des suites IKEv2

incluant des extensions post-quantiques, et intégration de HNDL dans le registre des risques officiel avec une valorisation financière documentée pour la présentation au COMEX.

HNDL et Conformité Réglementaire : Impact sur les Audits NIS 2

La prise en compte de la menace HNDL commence à apparaître dans les guides d'audit NIS 2. L'ANSSI, dans ses guides sectoriels publiés en 2025, mentionne explicitement l'analyse de risque quantique comme une composante attendue de la gestion des risques pour les entités essentielles. Cette évolution transforme HNDL d'un risque "futur et théorique" en un risque "présent et documenté" qui doit figurer dans le registre des risques de toute organisation soumise à NIS 2.

Concrètement, un auditeur NIS 2 peut désormais demander à voir : la liste des données sensibles avec durée de vie supérieure à 10 ans, leur niveau de protection cryptographique actuel, et la feuille de route de migration post-quantique de l'organisation. L'absence de toute réflexion sur ce sujet peut être notée comme une lacune dans la maturité de gestion des risques. Pour les entités importantes (NIB 2 niveau 2), cette lacune peut donner lieu à des recommandations d'amélioration ; pour les entités essentielles, elle peut donner lieu à des prescriptions formelles.

Vous pouvez consulter notre guide sur la conformité DORA 2026 et notre analyse de la mise en œuvre Zero Trust Microsoft 365 pour des perspectives complémentaires sur la conformité réglementaire en cybersécurité. Notre article sur la cryptographie post-quantique approfondit les aspects algorithmiques.

Liens Internes et Ressources Complémentaires

Pour approfondir les aspects techniques de la migration cryptographique post-quantique, consultez notre roadmap complète de migration post-quantique pour les DSI. Pour les aspects de conformité réglementaire associés, notre analyse de la conformité DORA 2026 et notre guide sur Zero Trust Microsoft 365 sont des lectures complémentaires utiles. L'article de référence du

NIST sur la cryptographie post-quantique est disponible sur csrc.nist.gov, et la documentation ENISA sur les menaces quantiques sur enisa.europa.eu.

Plan d'Action Anti-HNDL : Priorités Opérationnelles par Secteur

Voici les priorités d'action concrètes organisées par secteur d'activité, basées sur le niveau d'exposition HNDL et la maturité typique des organisations françaises dans chaque secteur.

Secteur santé : rechiffrement AES-256 des archives DPI en priorité 1, migration TLS hybride sur les systèmes d'information hospitaliers (SIH) en priorité 2, conformité avec les recommandations ANSSI/ANS pour les données de santé en priorité 3.

Secteur défense et aéronautique : systèmes sous exigences de conformité ANSSI/DGA — le calendrier est imposé réglementairement. Priorité immédiate : vérifier que tous les systèmes qualifiés ont une roadmap PQC validée par l'ANSSI, et que les communications inter-sites utilisent des solutions qualifiées post-quantiques ou en cours de qualification.

Secteur finance et assurance : les archives de transactions à valeur légale (5 à 10 ans selon les règles ACPR) sont particulièrement exposées. Migration TLS hybride en priorité 1 pour les plateformes de trading et les API interbancaires, rechiffrement des archives SWIFT en priorité 2.

Industries et R&D : identifier les 10 projets R&D les plus sensibles et protéger immédiatement leurs données de conception avec un chiffrement AES-256 sous clé ML-KEM. Migration TLS hybride sur les accès au dépôt de code source et aux systèmes PLM (Product Lifecycle Management) en priorité 1.

Indicateurs KPI pour Mesurer la Réduction du Risque HNDL

Pour piloter la réduction du risque HNDL dans le temps, il est important de disposer d'indicateurs mesurables. Ces KPI permettent de rendre compte à la direction et de prouver la progression de la maturité post-quantique.

KPI	Définition	Cible 2026	Cible 2028
% trafic TLS hybride	Sessions TLS avec ML-KEM / total sessions TLS	80%	99%
% archives rechiffrées	Archives sensibles rechiffrées AES-256 / total identifiées	50%	90%
Couverture inventaire crypto	Systèmes inventoriés / total systèmes en production	100%	100%
% HSM PQC-ready	HSM supportant ML-KEM / total HSM	30%	80%

Chaîne de Déchiffrement Post-Quantique : Étapes Techniques Détaillées

Pour comprendre pourquoi HNDL est une menace crédible et non théorique, il est utile de décrire précisément la chaîne technique que suivrait un attaquant disposant d'un CRQC. Cette analyse permet aussi d'identifier les points de rupture où des mesures défensives peuvent être efficaces.

Étape 1 — Récupération des échanges de clés capturés : l'attaquant extrait de ses archives les paquets TLS ClientHello et ServerHello qui contiennent les paramètres de l'échange de clés (la clé publique éphémère ECDH du serveur et celle du client). Pour RSA classique, ces archives contiennent directement le chiffré RSA de la clé de session PreMasterSecret.

Étape 2 — Application de l'algorithme de Shor : le CRQC exécute l'algorithme de Shor pour résoudre le problème du logarithme discret ECDH (ou la factorisation RSA). Pour ECDH sur P-256, cela requiert environ 2330 qubits logiques selon les estimations de Banegas et al. (2021). La durée d'exécution est estimée à quelques heures sur un CRQC idéal.

Étape 3 — Reconstruction de la session TLS : avec les clés de session (MasterSecret), l'attaquant peut dériver les clés de chiffrement de trafic (client_write_key, server_write_key) et déchiffrer l'intégralité du payload applicatif des sessions archivées. Le déchiffrement lui-même (AES-GCM) est très rapide sur du matériel classique.

Étape 4 — Exploitation des données : l'attaquant dispose maintenant des données en clair. Il peut rechercher par mots-clés, extraire des informations spécifiques, ou automatiser l'analyse avec des LLM pour traiter des volumes massifs d'archives en temps raisonnable. Des années d'emails d'entreprise, de transactions financières, ou de communications inter-ministérielles peuvent ainsi être analysées en quelques semaines.

Secteur Financier : Priorités HNDL pour les Banques et Assurances

Le secteur financier est particulièrement exposé à HNDL pour trois raisons : la haute valeur des données (transactions, positions, stratégies d'investissement), les obligations légales de conservation longue durée (5 à 10 ans pour les archives SWIFT et les journaux de transactions), et le niveau de sophistication des adversaires ciblant ce secteur (groupes APT financiers, services de renseignement économique).

Les **archives SWIFT** (messages MT103, MT202, etc.) chiffrées sur les 10 dernières années représentent un actif de renseignement économique de premier ordre. Les montants, les contreparties, les flux entre pays pourraient révéler des stratégies commerciales confidentielles, des contournements de sanctions, ou des flux financiers discrets entre entités liées. La migration des connexions SWIFT vers des algorithmes post-quantiques est une priorité absolue pour les établissements financiers.

Les **communications de trading haute fréquence** (HFT) sont moins exposées temporellement (les stratégies de trading deviennent obsolètes rapidement), mais les architectures d'infrastructure et les algorithmes propriétaires chiffrés dans les communications internes entre data centers pourraient révéler des secrets commerciaux à haute valeur. DORA impose d'ailleurs une analyse de risque technologique qui devrait intégrer la menace HNDL pour les établissements financiers significatifs.

Mon Opinion sur l'Urgence HNDL en 2026

Je vais être direct sur ce point : la quasi-totalité des PME et ETI françaises que nous rencontrons en 2026 n'ont aucun plan de réponse à HNDL. Elles savent que le problème quantique existe, elles l'ont lu dans des articles de presse, mais elles reportent l'action en se disant "ça n'arrivera pas avant 2035". C'est une erreur stratégique grave.

HNDL n'est pas une menace future : c'est une menace présente dont les effets sont différés. La collecte se fait maintenant. Si votre organisation a des données qui doivent rester confidentielles pendant 10 ans ou plus — et c'est le cas de la grande majorité des entreprises — alors votre adversaire a peut-être déjà une copie chiffrée de ces données dans ses archives. La migration post-quantique n'est pas une option, c'est une nécessité opérationnelle immédiate pour toute organisation responsable.

HNDL dans l'Industrie 4.0 et les Systèmes OT/ICS

Les environnements industriels (OT/ICS) présentent une exposition HNDL particulièrement préoccupante en raison des durées de vie très longues des équipements et des communications critiques qui y transitent. Un automate Siemens S7-1500 installé en 2022 sera probablement encore en production en 2035 ; les communications Profinet ou OPC-UA chiffrées captées aujourd'hui pourraient être déchiffrées à cette date avec des conséquences potentiellement catastrophiques pour la sécurité physique.

Les protocoles industriels chiffrés les plus exposés à HNDL incluent **OPC-UA** (qui utilise des certificats X.509 avec RSA/ECDSA), les **tunnels VPN IPsec** connectant les sites industriels au SI d'entreprise, et les **communications Modbus/TCP et DNP3 over TLS** déployées dans les smart grids. Pour ces protocoles, la migration PQC est particulièrement complexe car les équipements OT ont des cycles de mise à jour de firmware très longs (parfois plusieurs années) et des tests de qualification exigeants.

L'ANSSI recommande dans son guide ICS 2024 de prioriser la protection des communications OT/IT vers la DMZ industrielle, qui constitue le point de passage obligé des données vers les

systèmes d'information d'entreprise. Les **firewalls industriels** (Fortinet FortiGate Industrial, Check Point 1500D) peuvent être configurés pour effectuer une terminaison TLS hybride en proxy, offrant une protection PQC sans modifier les équipements OT en aval.

FAQ — Questions Fréquentes sur HNDL

HNDL est-il une menace réelle ou théorique en 2026 ?

La collecte de données chiffrées par des acteurs étatiques est documentée et avérée. Les révélations Snowden ont montré que la NSA pratiquait l'interception massive de trafic Internet depuis les câbles sous-marins. Des rapports des services de renseignement européens confirment que des acteurs chinois et russes font de même. HNDL est une menace active dès aujourd'hui — seul le déchiffrement reste futur.

HTTPS avec TLS 1.3 me protège-t-il contre HNDL ?

Non, si votre TLS 1.3 utilise uniquement des algorithmes classiques (ECDHE P-256, X25519). TLS 1.3 est le meilleur protocole de transport sécurisé classique, mais il reste vulnérable à HNDL tant que l'échange de clés utilise des algorithmes solubles par l'algorithme de Shor. Vous devez activer l'hybridisation ML-KEM sur votre TLS 1.3 pour protéger les communications futures.

Mes données dans le cloud sont-elles exposées à HNDL ?

Les données au repos chiffrées avec AES-256 par votre fournisseur cloud sont généralement sûres (AES-256 résiste aux attaques quantiques). La vulnérabilité principale concerne le transfert des données vers le cloud : si votre trafic TLS vers AWS/Azure/GCP utilise des algorithmes classiques, et qu'un adversaire l'a capturé, les données transmises sont potentiellement exposées. Les grands fournisseurs cloud migrent progressivement vers des algorithmes hybrides PQC sur leurs endpoints TLS.

Comment savoir si mes données ont déjà été collectées pour HNDL ?

Il est généralement impossible de savoir avec certitude si vos données ont été collectées dans le cadre d'un programme HNDL. La collecte passive est, par définition, invisible. Vous pouvez cependant évaluer votre exposition historique en identifiant quelles données sensibles transitaient en clair ou chiffrées avec des algorithmes classiques via des connexions Internet entre 2015 et aujourd'hui, et évaluer l'intérêt qu'elles représenteraient pour des acteurs étatiques.

VPN IPsec avec AES-256 me protège-t-il contre HNDL ?

Partiellement. Le chiffrement du payload avec AES-256 est post-quantique résistant. Mais l'échange de clés IKEv2 qui établit les clés AES utilise DH ou ECDH — vulnérable à l'algorithme de Shor. Si un adversaire a capturé le trafic complet de votre VPN (y compris les échanges IKEv2), il pourra dériver les clés AES et déchiffrer le payload une fois un CRQC disponible. La solution : activer les extensions IKEv2 post-quantiques (RFC 9370) sur vos équipements VPN.