Document ID: a3e9-threat-model
Author: Dennis DZ Zweigle
Version: June 2026

Classification: R&D – General Release

Summary

This document analyzes the Harvest Now Decrypt Later (HNDL) threat model, its implications for data security, and recommended strategies for post-quantum cryptographic migration.

Contents

Abstract

The "Harvest Now, Decrypt Later" (HNDL) attack model represents a structurally distinct threat category in which the act of data theft is temporally decoupled from the act of decryption. Adversaries intercept and archive encrypted network traffic today, holding it in reserve until a Cryptographically Relevant Quantum Computer (CRQC) can retroactively

break the underlying public-key algorithms. This threat is not theoretical: multiple Western intelligence agencies have confirmed that sophisticated nation-state actors are actively conducting HNDL operations against high-value targets. The data being harvested today may retain strategic, financial, or identity value for decades.

This paper analyzes the HNDL threat vector in depth, maps the regulatory timelines established by the NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) and NIST Interagency Report 8547, and details the A3E9 Virtual PKCS#11 Provider's hybrid cryptographic posture as the recommended enterprise response. The paper concludes with a sector-specific data longevity risk matrix and a phased enterprise readiness timeline aligned to CNSA 2.0 deadlines.

1. Introduction: A Breach That Happens in Reverse

Conventional cybersecurity incident response is organized around the moment of compromise. A breach is detected, contained, and remediated. HNDL undermines this model at its foundation. When an adversary intercepts TLS-encrypted traffic between two enterprise systems, the adversary has collected data that is, in the present moment, entirely unreadable. No alert fires. No integrity check fails. No anomaly is flagged. The encrypted payload is archived and held -- potentially indefinitely -- awaiting a future cryptanalytic capability that does not yet exist.

The concept is not new. Intelligence agencies have engaged in long-range signals collection for decades. What has changed is the credibility of the timeline. Quantum computing hardware has advanced materially: IBM has outlined a roadmap to deliver a fault-tolerant quantum system using approximately 10,000 physical qubits by 2029 [1]. Quantinuum, in collaboration with Microsoft, has demonstrated logical qubit error rates 800 times lower than corresponding physical qubit benchmarks [1]. Forrester Research's 2026 assessment explicitly characterized Q-Day as a plausible risk by 2030 [1]. Critically, three papers published between May 2025 and March 2026 reduced the estimated quantum resources required to break RSA-2048 from approximately 20 million qubits to fewer than one million, with some architectural proposals suggesting the attack might be achievable with as few as 100,000 qubits [1].

These are not proofs of imminent capability. They are demonstrations of a trajectory that has consistently surprised in the direction of accelerating risk. For organizations whose sensitive data must remain confidential through 2030 and beyond, the harvest is already occurring.

2. The HNDL Threat Vector: Mechanics and Scope

2.1. Three-Phase Attack Model

The HNDL attack model operates in three distinct phases [2]:

- **Phase 1: Harvest.** Adversaries collect encrypted information in transit through methods that exist today: intercepting network traffic at internet transit infrastructure, tapping undersea cables, compromising endpoints, or accessing cloud storage. The data is unreadable at the time of collection, making this phase entirely passive and effectively undetectable. The marginal cost of storing encrypted ciphertext is low; the potential future value is high.
- **Phase 2: Store.** The intercepted ciphertext is archived in large-scale data stores for years or decades. This phase may last until quantum decryption becomes feasible. There is no ongoing adversarial activity for defenders to detect during this period.
- **Phase 3: Decrypt.** When a CRQC capable of running Shor's algorithm becomes operational, the adversary retroactively decrypts the stored data. Classical public-key algorithms -- specifically RSA and Elliptic Curve Cryptography (ECC) -- are completely broken by this capability. The result is not a new breach. It is the delayed impact of data stolen years earlier.

"Encrypted data remains at risk because of the 'harvest now, decrypt later' threat in which adversaries collect encrypted data now with the goal of decrypting it once quantum technology matures. Since sensitive data often retains its value for many years, starting the transition to post-quantum cryptography now is critical to preventing these future breaches. This threat model is one of the main reasons why the transition to post-quantum cryptography is urgent." -- NIST Interagency Report 8547 [3]

2.2. The Lifespan Mismatch: The Core Risk Equation

The severity of HNDL exposure is not determined by whether a CRQC exists today. It is determined by the relationship between two independent variables: the data's sensitivity lifespan and the expected strength of the cryptography protecting it.

If data intercepted in 2026 must remain confidential through 2040, and a CRQC arrives in 2031, that data is already compromised -- regardless of whether the organization completes its PQC migration in 2035. The breach occurred at the moment of interception, not at the moment of decryption. Organizations cannot "unharvest" data that has already been collected.

This lifespan mismatch is the central analytical tool for prioritizing migration. The question is not "can a quantum computer break our encryption today?" The question is: "how long must this data remain confidential, and does that horizon extend beyond the expected strength of the algorithm protecting it?"

2.3. Threat Actor Profile

Open-source and governmental assessments describe HNDL activity primarily in the context of nation-state intelligence operations. The U.S. Department of Homeland Security, the UK National Cyber Security Centre, the European Union Agency for Cybersecurity (ENISA), and the Australian Cyber Security Centre have all issued post-quantum guidance premised on the assumption that sophisticated adversaries are currently collecting and storing sensitive

encrypted traffic for future decryption [1]. The National Endowment for Democracy has documented China's development of quantum computing infrastructure as an instrument of a data-centric strategic technology program with global security implications [1].

The 2026 Unit 42 Global Incident Response Report found that the fastest quartile of intrusions reached data exfiltration in 72 minutes in 2025, compared with 285 minutes in 2024. The share of incidents reaching exfiltration in under one hour increased from 19% in 2024 to 22% in 2025 [2]. This acceleration is directly relevant to HNDL: adversaries are collecting large volumes of data earlier in the attack cycle, consistent with a strategy of collecting now and sorting for value later.

3. Data Longevity Risk Matrix

The following matrix maps data categories to their typical sensitivity lifespan and the resulting HNDL risk posture. Organizations should use this matrix to prioritize which systems and data flows require immediate hybrid cryptographic protection.

Data Category	Typical Sensitivity Lifespan	Current Protection	HNDL Risk Posture
Diplomatic / Defense communications	20–50 years	RSA/ECDH TLS	**Critical -- Immediate action required**
Long-term identity credentials (PKI roots)	10–30 years	RSA/ECDSA	**Critical -- Immediate action required**
Tokenized asset signing keys	10–20 years	ECDSA P-256/P-384	**High -- Hybrid migration priority**
Financial transaction records	7–15 years	RSA/ECDH TLS	**High -- Hybrid migration priority**
Healthcare / genetic records	10–30 years	RSA/ECDH TLS	**High -- Hybrid migration priority**
Intellectual property / trade secrets	5–20 years	RSA/ECDH TLS	**High -- Hybrid migration priority**
Software signing certificates	5–10 years	RSA/ECDSA	**Medium -- CNSA 2.0 deadline: 2025/2030**
TLS session keys (ephemeral)	Session only	ECDH	**Low -- Forward secrecy limits exposure**

4. Regulatory Response: NIST and NSA Timelines

4.1. NIST IR 8547 and Algorithm Deprecation

NIST Interagency Report 8547 (Initial Public Draft, 2024) establishes a formal deprecation timeline for classical public-key algorithms across all NIST standards. RSA and ECC are scheduled for disallowance by 2035 [3]. This timeline is not aspirational guidance -- it

represents the formal end-of-life for the algorithms that underpin the vast majority of current enterprise PKI, TLS, and code signing infrastructure.

The three NIST FIPS standards finalized in August 2024 establish the approved replacements: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). These standards are the foundation for all enterprise PQC migration planning.

4.2. NSA CNSA 2.0: Binding Deadlines for National Security Systems

CNSA 2.0 (Version 2.1, December 2024) is the most operationally specific document in the U.S. government's PQC policy stack. It names exact algorithms, specifies exact parameter levels, and assigns binding deadlines by system category [4].

Approved Algorithms:

Function	Algorithm	Specification	Required Parameter
Key Establishment	ML-KEM	FIPS 203	ML-KEM-1024 (Level 5 only)
Digital Signatures	ML-DSA	FIPS 204	ML-DSA-87 (Level 5 only)
Firmware/Software Signing	LMS	NIST SP 800-208	SHA-256/192 (recommended)
Symmetric Encryption	AES	FIPS 197	AES-256
Hashing	SHA	FIPS 180-4	SHA-384 or SHA-512

Critical exclusions: ML-KEM-512, ML-KEM-768, ML-DSA-44, ML-DSA-65, and SLH-DSA (FIPS 205) are all explicitly prohibited for NSS use. Only Security Level 5 parameter sets are approved [4].

Transition Timeline:

System Category	Support and Prefer CNSA 2.0	Exclusively Use CNSA 2.0
Software/Firmware Signing	**2025 (past)**	2030
Web Browsers / Cloud Services	**2025 (past)**	2033
Networking Equipment (VPNs, routers)	**2026 (imminent)**	2030
Operating Systems	2027	2033
Niche/Custom Equipment	2030	2033
Legacy Systems	N/A	2035

By January 1, 2027, every new acquisition for a National Security System must support CNSA 2.0 algorithms or it cannot be deployed [4]. For organizations selling into classified environments, the planning phase is already over.

4.3. The Enterprise Migration Gap

The CNSA 2.0 deadlines create a direct tension with enterprise migration realities. For large organizations, realistic PQC migration timelines range from 12 to 15 or more years, depending on cryptographic complexity and system inventory [1]. An enterprise beginning a comprehensive PQC migration in 2026 may not complete it until 2038–2041 -- a period during which a CRQC could plausibly become operational. This gap is the primary driver for the hybrid cryptographic posture: organizations must begin protecting data in transit immediately, even before full hardware migration is complete.

5. A3E9 Recommended Posture: Hybrid Cryptography

Validation status for this section. What follows describes A3E9's design and its recommended posture, not a deployment record. Only SoftHSM2 and A3E9 Craton have been exercised against a real PKCS#11 module, and both are software: no hardware security boundary, no tamper detection, no dedicated cryptographic processor. The Thales, AWS CloudHSM and Utimaco vendor profiles are written and have never been executed against that vendor's hardware. liboqs is not a FIPS-certified module, A3E9 holds no CAVP or CMVP certificate and is not a validated cryptographic module, and SLH-DSA (FIPS 205) is not implemented - there is no request enum for it and no wired PKCS#11 mechanism. Per-case vector results and the current stated limits are published at https://a3e9.com/evidence.

5.1. Rationale for Hybrid Over Pure PQC

The NSA's CNSA 2.0 FAQ explicitly addresses the hybrid question. NSA's position is that hybrid constructions are acceptable during the transition period but are not a permanent end state -- the goal is exclusive use of CNSA 2.0 algorithms by the deadlines above [4]. However, for enterprises operating heterogeneous HSM environments where native FIPS 203/204 hardware support is inconsistent, hybrid is the only operationally viable posture today.

The hybrid approach provides two independent security guarantees: the classical algorithm provides security against current classical adversaries, and the PQC algorithm provides security against future quantum adversaries. Security holds if either algorithm remains unbroken. This is the correct posture for the current transition window.

5.2. The A3E9 HybridEnvelope Mechanism

The A3E9 Virtual Provider implements hybrid cryptography via the HybridEnvelope mechanism, defined in A3E9 Provisional Patent 64100,551. When a client application requests a signing operation, the A3E9 Normalization Engine intercepts the PKCS#11 C_Sign call and executes a dual-signing protocol:

1. **Classical Execution.** The payload is signed using the classical RSA or ECDSA key natively on the hardware HSM via the standard PKCS#11 C_SignInit / C_Sign sequence.

2. **PQC Execution. The payload is signed using the linked ML-DSA key identified by the CKA_LABEL suffix convention (e.g., prod-tls-cert-key -> prod-tls-cert-key-pqc). Where a vendor profile declares native ML-DSA support the operation is routed to that mechanism; where it does not, A3E9 executes the signature via the liboqs software fallback path, with the PQC private key read into host memory for the duration of the operation. The vendor routing named here is written but unvalidated - only the software modules SoftHSM2 and Craton have been exercised against a real module, and no Thales, AWS CloudHSM or Utimaco hardware path has been executed.**
3. **Composite Assembly.** The two signatures are concatenated into a CompositeSignatureValue ASN.1 structure per the IETF LAMPS Composite ML-DSA draft and returned to the application. The application is not required to be aware of the dual-signing operation.

5.3. Mapping A3E9 Posture to CNSA 2.0 Deadlines

The following table maps the A3E9 hybrid posture to the CNSA 2.0 transition timeline, providing a concrete enterprise readiness framework.

CNSA 2.0 Deadline	System Category	A3E9 Action Required
2025 (past)	Software/firmware signing, web/cloud	Deploy HybridEnvelope for all signing operations. Provision linked ML-DSA-65 or ML-DSA-87 keys per linked-key label convention.
2026 (imminent)	Networking equipment (VPNs, routers)	Enable hybrid key exchange (ML-KEM + ECDH) for all TLS sessions. Verify VendorProfile PQC capability flags for all HSM slots.
2027	Operating systems	Complete HSM firmware upgrades to native PQC-capable versions (Thales Luna 7.8.9+). Migrate liboqs fallback paths to native hardware where available.
2030	Exclusive use for software/networking	Disable classical-only signing paths in Normalization Engine. All signing operations must produce HybridEnvelope or pure ML-DSA output.
2033	Exclusive use for OS/browsers/cloud	Complete migration to pure PQC for all remaining system categories. Retire linked-key pairs; replace with standalone ML-DSA-87 keys.
2035	Legacy systems cutoff	All RSA and ECC operations disallowed per NIST IR 8547 deprecation schedule.

5.4. Strategic Advantages of the A3E9 Hybrid Posture

Immediate HNDL Mitigation. By deploying HybridEnvelope and ML-KEM key exchange today, organizations immediately neutralize the HNDL threat for data in transit. Any data encrypted under the hybrid construction requires a CRQC to break the ML-KEM component -

- which does not yet exist. The harvest is rendered cryptographically futile for data protected by the hybrid scheme.

FIPS Compliance Preservation. Because the classical algorithm (which is already FIPS 140-validated) remains in the critical path, the hybrid construction maintains current compliance posture while adding quantum resistance. This is essential for regulated industries where FIPS 140 validation is a contractual or regulatory requirement.

Vendor Agnosticism. The A3E9 VendorProfile matrix abstracts the uneven PQC readiness of the HSM market: the NONE capability flag routes PQC operations to the liboqs software fallback when hardware support is absent. That is a property of the profile mechanism, not a deployment record. The Thales, AWS CloudHSM and Utimaco profiles are written against published vendor documentation and have never been exercised against that vendor's hardware, and liboqs is not a FIPS-certified module.

Application Transparency. The HybridEnvelope mechanism operates entirely within the A3E9 Virtual Provider layer. The calling application issues a standard PKCS#11 C_Sign call and receives a composite signature. No application-level changes are required to achieve hybrid protection.

6. Open Questions and Active Investigation Areas

The following items represent areas where the A3E9 architecture's HNDL posture intersects with unresolved external factors:

1. **CRQC Timeline Precision.** The three 2025–2026 papers reducing RSA-2048 attack resource estimates to fewer than one million qubits are under active review by the cryptographic community. If these estimates hold, the Q-Day timeline may compress further, increasing urgency for the 2026 networking equipment deadline.
2. **CNSA 2.0 Hybrid Sunset.** NSA has indicated that hybrid constructions are a transition mechanism, not a permanent posture. The timeline for when NSA will require exclusive CNSA 2.0 use (rather than hybrid) in NSS is not yet formally specified beyond the category deadlines in Section 4.2.
3. **FIPS 140-3 Validation for PQC Modules.** As of July 2026, the CMVP validation pipeline for FIPS 203/204 implementations is active but not fully populated. The availability of FIPS 140-3 validated ML-KEM and ML-DSA modules will affect the timeline for retiring the liboqs software fallback path in favor of validated hardware.

References

[1] Cloud Security Alliance, "Harvest Now, Decrypt Later: Quantum Risk to AI Infrastructure," May 2026. https://labs.cloudsecurityalliance.org/research/ai-infrastructure-post-quantum-harvest-now-decrypt-later-v1/ [2] Palo Alto Networks Unit 42, "Harvest Now, Decrypt Later: Quantum Security Risk." https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl [3] National Institute of Standards and Technology, "Interagency Report 8547 (Initial Public Draft):

Transition to Post-Quantum Cryptography Standards," 2024. https://csrc.nist.gov/pubs/ir/8547/ipd [4] National Security Agency, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," Version 2.1, December 2024. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF [5] PostQuantum, "CNSA 2.0: The Complete Guide to NSA's Post-Quantum Requirements," May 2026. https://postquantum.com/cnsa-2-0/complete-guide/ [6] PQShield, "A Guide to CNSA 2.0 Compliant Cryptography Solutions," January 2025. https://pqshield.com/cnsa-2-0-compliant-crypto-solution/
