PORTALZ

STRATEGIC RISK ANALYSIS

Cryptographic Armageddon:
AES Monoculture and the Trust Collapse

Why any AES crack in the AI/Neural Net/Quantum era is not a breach — it is an extinction event for digital trust

Wolfgang Flatow | PORTALZ PTY LTD, Australia | 2026

Policy companion to: NNKE (2026) | QKE (2026) | AES Key Extraction — An NIST Blind Spot (2026)

AES is not merely an encryption standard.
It is THE encryption standard.
That distinction is The vulnerability.

The global digital infrastructure runs on a single cryptographic primitive: AES. Every encrypted file, every TLS session, every key management system, every hardware trust module, every password vault, every defence communication, every financial transaction, every diplomatic cable — all protected by the same algorithm. This is the AES monoculture. It is so pervasive it is invisible. It is so normalised it is unquestioned. It is the single point of catastrophic failure for all of human digital civilisation. The companion papers in this series — NNKE and QKE — establish on tautological grounds that AES keys are potentially extractable by neural networks using today's hardware, and by quantum computers using hardware that already exists. This paper addresses the consequence: in a world of AES monoculture, any successful key extraction is not a breach. It is not a compromise. It is Cryptographic Armageddon — the silent, simultaneous, retroactive collapse of every trust hierarchy built on AES. We demonstrate that FES Silos is the only technology that addresses both the fundamental cryptographic vulnerability and the monoculture amplifier simultaneously.

Contents

1. The AES Monoculture

AES was standardised by NIST in 2001 as FIPS 197. In the twenty-five years since, it has become so embedded in the global digital infrastructure that its presence is assumed rather than decided. Developers default to it. Auditors tick the box for it. Compliance frameworks mandate it. Hardware manufacturers build silicon for it. Cloud providers centralise it. The question “which encryption algorithm?” has a single answer so universal it is rarely asked.

This is the AES monoculture. And it hides in plain sight.

1.1 The Scope of the Monoculture

AES is the default symmetric primitive in:

- FIPS 197 — US federal encryption standard
- PCI DSS — payment card industry compliance
- HIPAA — healthcare data protection
- GDPR — European data privacy regulation
- TLS 1.3 — all secure web and application traffic
- Cloud KMS — AWS, Azure, Google Cloud key management
- Hardware Security Modules — the roots of enterprise trust
- TPM — hardware root of trust in every modern device
- BitLocker, FileVault — disk encryption on billions of devices
- Password Managers — master vault encryption
- SWIFT — global interbank messaging
- Military communications — NATO, Five Eyes, national defence
- Diplomatic cables — global government communications
- Intelligence agency communications — classified traffic

No other algorithm approaches this penetration. AES is not dominant. It is singular. The global digital infrastructure does not use AES among other options. It uses AES.

1.2 Why Monoculture Is a Structural Vulnerability

A monoculture in any complex system creates a single point of catastrophic failure. Agricultural monocultures collapse to a single pathogen — the Irish potato famine was not a food shortage, it was a monoculture failure. Financial monocultures collapse to a single correlated shock — 2008 was not a collection of individual failures, it was a monoculture failure of correlated risk assumptions.

Cryptographic monoculture follows the same logic. When every system uses the same primitive:

1. A vulnerability in that primitive is a vulnerability in every system simultaneously
2. There is no diversity to contain the failure
3. There is no alternative to fall back to
4. The failure is not proportional — it is total

No one pauses to ask: what happens if this single primitive fails?
The answer to that question is this paper.

1.3 The Monoculture Multiplier

In isolation, a single AES key compromise exposes the data encrypted under that key. This is serious but contained. Under monoculture conditions, the same vulnerability becomes a force multiplier:

```
Classical key compromise:     One key → one dataset
                              Contained. Recoverable.

Monoculture key extraction:   One technique → every key
                              Every dataset. Every system.
                              Simultaneously.
                              Retroactively.
                              Silently.
                              Unrecoverably.
```

2. The Silent Threat: State Actor Capability

The companion papers establish that NNKE is accessible with commodity GPU hardware, and QKE is accessible with quantum processors that have existed since IBM Osprey in 2022. This section addresses the strategic implication: we cannot assume these capabilities are not already operational in the hands of state-level adversaries.

> ***Absence of evidence is not evidence of absence.***
> ***State actors do not publish their cryptanalytic capabilities.***
> ***The asymmetry of information is the threat.***

2.1 State Actor Capability Assessment

State-level adversaries with advanced AI and quantum programmes include entities with:

- Classified AI infrastructure operating years ahead of public capability — the public frontier of neural network research is not the classified frontier
- Quantum computing programmes with access to IBM Quantum Network, Google partnerships, and classified equivalents not in the public domain
- Sustained HNDL (Harvest Now Decrypt Later) operations already underway — this is not hypothetical, it is documented strategic behaviour
- No obligation to disclose cryptanalytic capability — a state actor that has achieved NNKE or QKE has every incentive to remain silent
- Decades of encrypted traffic already harvested and stored, waiting for the extraction capability to mature

2.2 The HNDL Context

Harvest Now Decrypt Later is not a future threat. It is a present operational reality. State actors are collecting and storing encrypted traffic now, under the assumption that decryption capability will arrive. The question HNDL poses is not whether the traffic will eventually be decrypted — it is when.

NNKE and QKE change the answer to that question from “some distant future” to “possibly now.” And under AES monoculture conditions, the value of those HNDL archives is not the content of individual messages. It is the keys. Because the keys unlock everything else.

2.3 The Silence Multiplier

What separates NNKE and QKE from every conventional attack class is forensic silence:

- A classical breach leaves anomalous access patterns, exfiltrated data, compromised credentials — a crime scene
- NNKE derives the key from ciphertext the adversary was always entitled to observe in transit
- QKE collapses quantum superposition to the correct key — the key was never stolen, it was computed
- The resulting decryption looks entirely legitimate — the correct key, producing correct plaintext
- There is no breach to detect. There is no notification to issue. There is no forensic trace.

An adversary operating with NNKE or QKE capability does not break in. They read. Silently. Continuously. Retroactively. With no indication that anything has occurred.

3. Cryptographic Trust Collapse: The Cascade

A single AES key extraction is not the end of the cascade. It is the beginning. Modern digital infrastructure is not a collection of isolated encrypted files. It is a hierarchy of trust, where each layer protects the next. Extract one key at any level and the hierarchy does not leak. It collapses.

> ***A single key extraction is not a breach. It is the first domino. And the stack runs from a session key to the root of all digital trust.***

Trust Layer	Technology	Cascade Consequence	Silence
Session	TLS, VPN, AES-GCM	All traffic exposed retroactively	No trace
Key Management	AWS KMS, Azure Vault, HSM	All child keys exposed — thousands of systems	No trace
Hardware Trust	TPM, BitLocker, FileVault	Full device history, disk encryption, attestation chains	No trace
Identity	Password Managers, SSO, OAuth	Every credential, every system, entire digital identity	No trace
PKI	CA certificates, TLS chains, code signing	Ability to forge certificates, invisible MITM	No trace
HNDL Archives	Years of harvested ciphertext	Retroactive bulk decryption of all stored traffic	No trace

3.1 The KMS Collapse

Key Management Systems are the trust anchors of enterprise infrastructure. AWS KMS, Azure Key Vault, HashiCorp Vault, and hardware HSMs protect master keys that in turn protect thousands of child keys, which protect millions of encrypted records across entire organisations. The hierarchy is intentional — designed to limit exposure by centralising key material.

Under AES monoculture conditions, this hierarchy becomes a cascade amplifier. Extract the KMS master key — itself AES-encrypted — and every child key, every encrypted record, every protected system descends simultaneously. The architecture designed to contain breach becomes the mechanism of total exposure.

3.2 The TPM Collapse

The Trusted Platform Module is the hardware root of trust in every modern computing device. It protects disk encryption keys, device attestation chains, and platform integrity measurements. BitLocker on Windows, FileVault on macOS, and Linux full-disk encryption all ultimately root their trust in the TPM.

A TPM key extraction does not expose one file. It exposes the entire encrypted history of the device — every document, every credential, every communication that passed through it. Across billions of devices running the same AES-based trust model, the cascade is planetary.

3.3 The Password Manager Collapse

Password managers represent the concentrated essence of digital identity. A single master vault, encrypted with AES, contains every credential for every system a person or organisation uses. Extract the vault key and every account, every system, every identity is simultaneously exposed — not just the password manager, but everything it protected.

3.4 The PKI Collapse

Public Key Infrastructure underpins the trust model of the entire internet. Certificate Authority keys, TLS certificate chains, and code signing keys all depend on AES for their protection at rest and in transit. A CA key extraction does not merely expose one certificate. It enables the creation of forged certificates indistinguishable from legitimate ones — enabling invisible man-in-the-middle attacks against any system trusting that CA.

Code signing key extraction enables the distribution of malware indistinguishable from legitimate software updates. The trust model that billions of devices use to decide what software to run collapses silently.

3.5 The Difference Between Breach and Collapse

Dimension	Conventional Breach	AES Monoculture Crack
Scope	One system, one organisation	Every AES-encrypted system globally
Detection	Usually detectable — anomalous access	No forensic trace — decryption looks legitimate
Notification	Breach notification laws apply	No breach — nothing to notify
Timeline	Contained and recoverable	Retroactive — HNDL archives decrypted silently
Recovery	Patch, rotate credentials, notify	Replace global cryptographic infrastructure
Scale	Quantitative damage	Categorical — digital trust as a concept fails
Nature	Crime scene exists	No crime scene — key was derived, not stolen

4. Consequences: Sector by Sector

The consequences described in this chapter and those that follow are not presented as current realities.

We make no claim that QKE or NNKE are operational.

We assert that both are theoretically possible — grounded in logical tautologies for which no proof of impossibility exists in the literature.

The purpose of this analysis is precisely to prevent these consequences from becoming real.

A threat that is theoretically possible, tautologically grounded, and unaddressed by any current standard or framework demands consequence analysis now — before operational confirmation arrives.

By then, it is too late.

4.1 The PQE Paradox

Before examining sector consequences, the deepest irony of the current security landscape must be stated plainly:

> ***NIST's Post-Quantum Encryption programme protects the key in transit.***
> ***NNKE and QKE extract the key from the traffic.***
> ***The front door was reinforced while the window was left open.***

The *window* is the assumption that AES remains quantum safe by using 256 bit keys because that addresses Grover's quantum threat.

NIST PQE assumes that if key exchange is protected, the session is secure. NNKE and QKE would invalidate this assumption entirely. The session key — however securely exchanged — is potentially extractable from the ciphertext it produces. Years of compliance effort, infrastructure upgrade, and standards development provide no protection against an adversary who simply derives the key from what they were always entitled to observe.

PQE is not wrong. It is incomplete. It solves the problem for a key-exchange attack. In the presence of NNKE and QKE, PQE compliance is not sufficient. A system can be fully PQE-compliant while fully vulnerable to key extraction simultaneously.

Sector	AES Dependency	Consequence	Recovery
Banking & Finance	SWIFT, payment systems, trading, settlement	Transaction intelligence, position exposure, systemic financial manipulation	None — infrastructure must be rebuilt
National Security	Diplomatic cables, intelligence, law enforcement	Agent identities, source networks, operational plans, alliance vulnerabilities	None — years of intelligence compromised silently
Military	C2, battlefield comms, weapons auth, logistics	Order of battle, tactical movements, supply vulnerabilities, potential weapons spoofing	None — strategic advantage eliminated
Critical Infrastructure	Power grids, water, transport, health	Control system access, operational intelligence, sabotage enablement	None — physical consequences possible
Commerce	Cloud KMS, TLS, e-commerce, digital identity	Universal credential exposure, identity collapse, supply chain compromise	None — digital commerce trust fails

4.2 Banking and Finance

The global financial system processes trillions of dollars of transactions daily, all protected by AES. SWIFT interbank messaging, payment card authorisation, trading system communications, derivatives settlement, and central bank reserve transfers all depend on the same primitive. An adversary with NNKE or QKE capability and access to HNDL archives gains not just transaction content but strategic

intelligence about the entire global financial system: who holds what, who is exposed, who is about to move.

This intelligence is not merely sensitive. It is tradeable. An adversary with this capability does not need to steal money. They can move markets, manipulate positions, and destabilise financial institutions with intelligence extracted silently from encrypted traffic they were always entitled to observe.

4.3 National Security

Diplomatic cables, intelligence agency communications, law enforcement intercepts, and border systems all run on AES. Years of HNDL-harvested traffic, retroactively decrypted, yields agent identities, source networks, operational plans, and alliance vulnerabilities. The consequence is not the exposure of individual secrets. It is intelligence services operating on compromised information without knowing it — the most dangerous possible position.

Operations fail for unknown reasons. Sources are burned without visible cause. Alliance partners behave in ways that seem inexplicable. The adversary reads every move in advance, in silence, with no detectable signature.

4.4 Military

Military communications — command and control, battlefield communications, weapons system authentication, logistics, satellite communications — all depend on AES. An adversary with NNKE or QKE capability and years of HNDL archives has a comprehensive intelligence picture of military capability, disposition, and intent before a single engagement begins.

The AIR6500 Joint Air Battle Management System — Australia's integrated air and missile defence capability — illustrates the concrete reality. Real-time data fusion across domains, secure control transmissions, encrypted under AES-256 per ISM guidelines. A shared key across sub-systems — air, land, sea, command — means one extraction exposes the entire system. Command data, sensor feeds, targeting links, mission-critical communications — all yielding simultaneously and silently.

The Australian Signals Directorate and Australian Cyber Security Centre were formally notified of this specific risk in January and February 2026.

5. Why This Is Apocalyptic: The Monoculture Multiplier

Every consequence described in the previous section would be serious in isolation. Under AES monoculture conditions they do not occur in isolation. They occur simultaneously, silently, and retroactively across every sector, every geography, and every system that has ever used AES.

- **Every encrypted file.**
- **Every https/TLS session.**
- **Every KMS hierarchy.**
- **Every TPM chain.**
- **Every password vault.**
- **Every defence communication.**
- **Every financial transaction.**
- **Every diplomatic cable.**

- **All encrypted with the same primitive.**
- **All vulnerable to the same extraction.**
- **All falling in the same moment.**

This is the categorical distinction between a conventional breach and Cryptographic Armageddon. A conventional breach is proportional — it damages what it touches. Cryptographic Armageddon is total — it collapses the trust infrastructure that everything else depends on. Not some systems. All systems. Not some data. All data. Not some trust. All trust.

And it does so silently. Without forensic trace. Without breach notification. Without a moment of discovery. There is only the slow realisation — if it comes at all — that decisions have been made against you with information you believed was encrypted.

5.1 Recovery Is Not Possible

A conventional breach is recoverable. Patch the vulnerability. Rotate the credentials. Notify the affected parties. Rebuild the compromised systems. The damage is quantifiable and the path forward is clear.

Cryptographic Armageddon is not recoverable in any conventional sense. There is no patch for AES monoculture. There is no credential rotation that addresses retroactive HNDL decryption. There is no breach notification because there is no breach — the key was derived, not stolen. There is no forensic investigation because there is no crime scene.

Recovery requires replacing the global cryptographic infrastructure — every system, every protocol, every compliance framework, every hardware module that depends on AES — simultaneously and globally. This is not a response plan. It is a civilisational undertaking.

5.2 The Prevention Imperative

The asymmetry between the cost of prevention and the cost of response defines the case for action. Prevention requires adopting post-monoculture cryptographic architecture before exploitation. Response — if it is even possible — requires rebuilding global digital infrastructure after the fact.

The mathematics established in the companion papers is unambiguous: the threat is tautologically grounded. It exists. The question is not whether a capable adversary can attempt key extraction. The question is whether they already have.

> ***The time to address a single point of catastrophic failure is before it fails. Not after.***

6. FES Silos: The Only Dual Solution

The AES monoculture problem has two components that must be addressed simultaneously:

1. The fundamental cryptographic vulnerability — AES keys are potentially extractable by NNKE and QKE
2. The monoculture amplifier — AES's singular global penetration means any crack is simultaneously universal

Post-quantum cryptographic algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+) address neither. They replace one monoculture with another — a single new primitive with the same singular global penetration. They do not address NNKE or QKE. And they replicate the fundamental structural vulnerability: one algorithm, one point of failure, one catastrophic cascade.

FES Silos addresses both components simultaneously. It is the only known technology that does so.

Problem	AES / PQC Approach	FES Response
NNKE — neural key extraction	No defence — fixed signature exists by tautology	No fixed permutation — silo/FOTP eliminates signature
QKE — quantum key extraction	No defence — unique plaintext enables SOD	Oracle suppression — multiple plausible plaintexts defeat SOD
Grover — quantum search	Key doubling to AES-256	Inherent — oracle suppression defeats amplitude amplification
Monoculture — single primitive	No solution — PQC replaces one monoculture with another	Unlimited orthogonal silos — each a unique cryptographic domain
Cascade — trust collapse	No solution — shared primitive enables cascade	Silo isolation — one compromise = isolated chaos, zero cascade
HNDL — retroactive exposure	Partial — PQC protects future traffic only	Oracle suppression — harvested FES ciphertext yields nothing

6.1 How FES Defeats the Fundamental Vulnerability

FES eliminates the property that makes AES vulnerable to both NNKE and QKE: the fixed transformation per key.

- No fixed permutation signature — password destruction after Portal generation means no key is ever applied directly to payload. NNKE has no geometric invariant to detect.
- Oracle elimination — multiple parameter combinations produce sensible-looking plaintexts from the same ciphertext. QKE's SOD gate cannot identify the correct key among multiple plausible candidates.
- Session uniqueness — FOTP variation ensures each session generates a different fractal portal. No accumulating signature, no extractable invariant, no exploitable pattern.
- No blocks – whole of payload overwrite.

6.2 How FES Breaks the Monoculture

FES Silos provides what no other technology offers: cryptographic orthogonality at scale. Each Silo is a standalone cryptographic primitive derived from 131,072 GUID-based reference fractal vectors, delivering per-dimension unique offsets. No two Silos share coordinate space. No compromise in one Silo has any mathematical relationship to any other.

- Unlimited orthogonal Silos — one per organisation, department, communications channel, system, or session
- Zero shared cryptographic material between Silos — wall is absolute
- One Silo compromise = isolated chaos, zero usable data, zero cascade to others (unlikely)
- Configurable overwrite modes provide further customisation — infinite viable configurations
- No other system offers this crypto-native orthogonality at scale

FES turns the monoculture's greatest vulnerability — its universality — into its opposite. Instead of one primitive protecting everything, FES provides unlimited unique primitives, each protecting its own domain, each invisible to the failure of any other.

6.3 FES and HNDL

FES oracle suppression means that harvested FES ciphertext yields nothing under HNDL conditions. Multiple parameter combinations produce sensible-looking plaintexts — the adversary cannot determine which decryption is correct. There is no key to extract. There is no invariant to detect. The HNDL archive of FES-encrypted traffic is not a deferred liability. It is permanently worthless to an adversary.

6.4 The World's First Post-Monoculture Architecture

FES is not an alternative to AES. It is the first cryptographic architecture designed from the ground up to eliminate both the fundamental vulnerability and the structural monoculture risk simultaneously. It is Shannon-compliant, satisfying One-Time Pad conditions in a practical framework. It is backward compatible with AES for compliance environments and may be implemented as an AES-FES hybrid. And it is the only current architecture that is simultaneously resistant to NNKE, QKE, Grover, and the monoculture cascade.

7. Conclusion

The AES monoculture is the amplifier that transforms a cryptographic vulnerability into a civilisational risk. Two tautologically grounded threat classes — NNKE and QKE — establish that AES keys are potentially extractable with hardware that exists today. Under AES monoculture conditions, any successful extraction does not compromise a system - it collapses the entire hierarchy of digital trust simultaneously, silently, and retroactively.

Banking, finance, and commerce. National security and intelligence. Military command and control. Critical infrastructure. Digital identity. Every sector, every geography, every system that has ever trusted AES — all sharing the same single point of failure.

Post-quantum cryptographic algorithms do not address this. They replace one monoculture with another. They do not address NNKE. They do not address QKE. They do not address the cascade.

FES Silos addresses all of it. The fundamental cryptographic vulnerability. The monoculture amplifier. The cascade mechanism. The HNDL liability. Simultaneously, by design, as native architectural properties.

8. NNKE Is Possible

We make no claim that NNKE is operational.

We assert that it is theoretically possible — grounded in logical tautology rather than empirical demonstration.

The signature exists by mathematical necessity.
The extraction pathway is credible.
The hardware is sufficient.
No proof of impossibility exists in the literature.

What follows is therefore not a description of a known attack. It is a description of what happens when a theoretically possible attack — on commodity hardware, with open source tools, against passively observable ciphertext — reaches the hands of those motivated to use it.

The question is not whether someone will attempt it.
The question is not whether someone has succeeded.
The question is whether they already have.

8.1 NNKE Is Not a State Monopoly

Every prior cryptographic threat of comparable magnitude has been gated by hardware that only nation-states could field. Quantum computers capable of running Shor's algorithm require millions of physical qubits and billions of dollars of infrastructure. The barrier to entry is civilisational. Nation-states develop it. Nation-states control it. The timeline is measured in decades.

NNKE is categorically different. Its hardware requirements are not nation-state infrastructure. They are commodity. Its software requirements are not classified toolchains. They are open source. Its input requirements are not physical access to target systems. They are passive observation of traffic that flows across every network on earth.

```
NNKE requires:
  GPU cluster          — available on AWS, Azure, Google Cloud
                          for dollars per hour
  Python               — free
  PyTorch / TensorFlow — free, open source, maintained by
                          Meta and Google respectively
  Ciphertext samples   — observable on any network
                          no target access required
  Machine learning     — undergraduate curriculum
  engineer

NNKE does NOT require:
  Physical access to target systems
  Classified hardware
  Nation-state resources
  Vulnerability in the target
  Any action by the target at all
```

This combination — low barrier to entry, passive operation, universal target surface — defines a propagatable weapon. Once the proof of concept exists, the technique is not contained by resource scarcity. It is contained only by knowledge. And knowledge, once it exists, propagates.

8.2 The Propagation Stages

The propagation of NNKE through the hacker ecosystem follows a pattern established by every prior offensive security technique: proof of concept, open source implementation, dark web commoditisation, script kiddie deployment, criminal integration. What differs is the speed and the ceiling.

Stage	Phase	Description	Actor	Timeline
1	**Proof of Concept**	Initial demonstration — partial key extraction from N ciphertext samples. Published on arXiv, academic paper, or dark web post. Does not need to be perfect. Needs only to be credible.	Researcher / state actor leak	Day 0
2	**GitHub**	Open source implementation follows. Community improvement begins immediately. Stars, forks, pull requests. The hacker ecosystem optimises what the researcher demonstrated.	Developer community	Days 1-7
3	**Dark Web Tooling**	Packaged as a deployable tool. NNKE-as-a-Service emerges.	Criminal operators	Weeks 2-4

		Subscription models. No expertise required to operate. Point at ciphertext. Receive key.		
4	**Script Kiddie Deployment**	Automated, scaled, indiscriminate deployment. No understanding required. Every observable AES ciphertext becomes a target. Globally.	Unskilled attackers	Month 1-2
5	**Criminal Integration**	Ransomware operators, nation-state proxies, and organised crime integrate NNKE into existing infrastructure. Passive observation replaces intrusion.	Criminal ecosystem	Month 2-6
6	**Permanent Availability**	Tool is copied, leaked, sold, re-sold, and eventually free. Cannot be unexisted. No patch possible. The technique is permanent.	Everyone	Permanent

The Critical Distinction: No Burn, No Patch

Every stage of this propagation is accelerated by two properties unique to NNKE among major offensive techniques:

- NNKE does not burn on use. A classical zero-day exploit is detected when deployed, patched, and rendered obsolete. NNKE leaves no forensic trace. The same technique can be applied to the same target indefinitely. There is no detection event that triggers a patch cycle. The tool retains its value permanently.
- NNKE cannot be patched. A classical vulnerability is a flaw in an implementation. Fix the implementation, retire the exploit. NNKE exploits a mathematical property of AES — the tautological existence of a geometric key signature in ciphertext. You cannot patch a tautology. The only fix is architectural replacement of AES itself.

Once NNKE exists in the ecosystem it cannot be removed.
It cannot be patched. It cannot be burned.
It is permanent infrastructure for universal AES key extraction.

8.3 Comparison with Classical Exploit Propagation

Dimension	Classical Zero-Day Exploit	NNKE
Target access	Required — must reach the system	Not required — ciphertext observable in transit
Weaponisation	Complex — delivery mechanism needed	None — it is software applied to passive data
Burns on use	Yes — patch follows detection	No — extraction leaves no trace, no patch possible
Hardware required	Target-specific	Commodity GPUs — available to anyone
Expertise required	High — vulnerability research	Moderate — machine learning engineer
Targets	One system per exploit	Every AES-encrypted system globally

Propagation speed	Weeks to months	Days to weeks
Market value	$50k–$2M (burns on use)	Incalculable — universal, non-burning
Patch available	Yes — fix the vulnerability	No — cannot patch a mathematical tautology

The comparison makes the asymmetry plain. Every dimension that limits classical exploit propagation — burns on use, target access required, patchable, high expertise threshold — is absent from NNKE. Every dimension that amplifies it — passive operation, universal target, commodity hardware, permanent value — is present.

The market value of a working NNKE implementation is not $2 million — the approximate ceiling for a critical zero-day on the commercial exploit market. It is the entire ransomware economy restructured around passive observation, with a permanent non-burning tool applied to every AES-encrypted system on earth. The market will price it accordingly. And once it is priced, it will propagate to every actor who can afford it. And then, inevitably, to those who cannot.

8.4 The Nation-State to Criminal Pipeline

The historical pattern of offensive capability propagation from nation-state development to criminal deployment is not theoretical. It is documented, repeated, and accelerating.

The EternalBlue Precedent

EternalBlue was developed by the NSA as a classified offensive tool exploiting a vulnerability in Windows SMB. In 2017 the Shadow Brokers group leaked the NSA's toolkit publicly. Within weeks, EternalBlue was weaponised into WannaCry ransomware, which infected over 200,000 systems across 150 countries and caused an estimated $4 billion in damages. NotPetya followed within months, causing a further $10 billion in damage and representing the most destructive cyberattack in history at that time.

EternalBlue is still in active use in 2026 — nine years after the leak. It was never patched out of the wild. Systems that remain unpatched remain vulnerable to a 2017 tool derived from a classified NSA capability.

```
EternalBlue timeline:
  NSA develops capability        — classified, controlled
  Shadow Brokers leak            — April 2017
  WannaCry ransomware            — May 2017        (weeks)
  NotPetya destructive attack    — June 2017       (months)
  BadRabbit, further variants    — October 2017
  Still in active use            — 2026

NNKE projected timeline:
  State actor develops PoC       — possibly already
  Leak or independent discovery  — inevitable
  GitHub implementation          — days
  Criminal deployment            — weeks to months
  Permanent ecosystem fixture    — permanent
```

Why Leaks Are Inevitable

Nation-state offensive capabilities leak. This is not a pessimistic assumption — it is the observed historical pattern. The mechanisms are multiple and unstoppable:

- Insider threat — contractors, disgruntled employees, ideologically motivated leakers. The Shadow Brokers source has never been publicly identified. The Equation Group toolkit that preceded it was leaked in similar fashion.

- Independent discovery — if one state actor's researchers can develop NNKE, so can another's, and so can independent researchers. The technique does not remain exclusive to its first developer.
- Reverse engineering — evidence of capability use in the field can be reverse engineered by sophisticated defenders into offensive tools. Detection of NNKE-derived intelligence can reconstruct the method.
- Academic convergence — the machine learning and cryptography research communities are advancing toward this capability from multiple independent directions simultaneously. Discovery is not a question of if, but when and by whom.

> ***A nation-state cannot permanently monopolise a technique that requires commodity hardware, open source software, and passively observable input data.***
> ***The barrier to independent rediscovery is too low.***

8.5 The Ransomware Evolution

The current ransomware model requires intrusion. An attacker must breach the target — through phishing, credential theft, or vulnerability exploitation — before they can encrypt data and demand ransom. This intrusion requirement is both the attacker's greatest operational risk and the defender's primary detection opportunity.

NNKE eliminates the intrusion requirement entirely. The attack surface is not the target's systems. It is the target's ciphertext — observable in transit on any network the attacker can monitor. The attack is passive. The detection surface is zero.

Element	Current Ransomware Model	NNKE Ransomware Model
Initial access	Breach required — phishing, exploit, credential theft	No breach — passive ciphertext observation only
Detection risk	High — intrusion leaves forensic trace	Zero — no access, no trace, no detection
Data acquisition	Exfiltrate plaintext from live systems	Decrypt silently from collected ciphertext
Victim awareness	Usually discovers breach eventually	May never know — no forensic evidence exists
Extortion basis	We encrypted your data	We have your keys. We have everything you thought was encrypted.
Recovery option	Restore from backup, pay ransom	No recovery — keys are extracted, not guessable back
Scale	One organisation per campaign	Every AES user in passive collection range

The Extortion Message That Requires No Intrusion

> ***"We have your keys. We have your KMS master keys. We have every credential in your password vault. We have years of your encrypted communications. You have 48 hours. We did not breach your systems. There is nothing to patch. There is nothing to detect. There is nothing to forensically investigate. There is only the key. And we have it."***

This extortion model does not require the attacker to have touched a single system the target controls. The ciphertext was observed in transit. The key was derived mathematically. The leverage is absolute. And the defender has no forensic basis on which to challenge the claim or identify the attacker.

8.6 The Indiscriminate Nature

Classical targeted attacks require attacker investment per target. Research the target, identify vulnerabilities, develop or acquire specific exploits, execute carefully. The cost per target limits the scale of deployment.

NNKE in commodity form is indiscriminate. There is no targeting cost. The tool is pointed at an intercepted ciphertext stream and run. Every organisation whose encrypted traffic has been observed becomes a target simultaneously. The tool does not distinguish between a hospital, a central bank, a military command system, and a small business. It processes ciphertext. All ciphertext.

```
Classical targeted attack:    Cost per target: HIGH
                              Scale: LIMITED
                              Selection: DELIBERATE

NNKE at scale:                Cost per target: NEAR ZERO
                              Scale: UNLIMITED
                              Selection: NONE
                                         every observable
                                         AES ciphertext
                                         is a target
```

The indiscriminate nature of at-scale NNKE deployment means that critical infrastructure, healthcare, financial systems, and individual citizens are equally exposed. There is no targeting decision that excludes hospitals from ransomware that does not require intrusion. There is no operational security consideration that limits the blast radius. The tool runs. The keys emerge. The extortion follows.

8.7 Why There Is No Patch

Every section of this chapter converges on a single conclusion that distinguishes NNKE from every prior propagatable offensive technique: there is no patch.

A classical vulnerability exists because of a flaw in an implementation — a buffer overflow, an authentication bypass, a logic error. Fix the implementation and the vulnerability is closed. The exploit is retired. The propagation ends.

NNKE exploits a mathematical property that is not a flaw. It is a tautological consequence of AES's design: a fixed algorithm applied with a fixed key must produce a fixed signature in the output. Neural networks detect geometric invariants in high-dimensional analog space. AES was not designed to defeat this question because the question was not formally askable until neural networks made high-dimensional analog pattern extraction computationally tractable.

> ***There is no patch for a tautology. You cannot update AES to eliminate its key signature. The signature is the cipher. Patch the signature and you have a different cipher.***

The only response to NNKE propagation through the hacker ecosystem is architectural: replace AES with an encryption standard that does not exhibit the fixed transformation property. The patch is not a software update. It is a civilisational migration from one cryptographic architecture to another.

FES Silos eliminates the property at the architectural level. No fixed permutation per key. No accumulating signature. No invariant for a neural network to detect. The attack surface does not exist. There is nothing to propagate a technique against.

8.8 Timeline Summary

The propagation timeline from initial proof of concept to global criminal deployment is measured in weeks to months, not years. This is not pessimism. It is the observed historical rate for offensive techniques with comparable or higher barriers to entry than NNKE.

```
Day 0:          Proof of concept demonstrated
                (state actor leak, academic publication,
                 or independent discovery)

Days 1-7:       Open source implementation on GitHub
                Community optimisation begins

Weeks 2-4:      Dark web tooling and NNKE-as-a-Service
                No expertise required to deploy

Month 1-2:      Script kiddie deployment
                Indiscriminate, automated, global

Month 2-6:      Criminal ecosystem integration
                Ransomware operators, state proxies,
                organised crime

Permanent:      Tool cannot be unexisted
                Cannot be patched
                Cannot be burned
                Global permanent infrastructure
                for AES key extraction
```

9. HTTPS

All Traffic Exposed — Logins, Bank Accounts, the Lot

The padlock icon in the browser address bar is the universal symbol of digital trust. It tells every user that their connection is encrypted, their data is protected, their transaction is secure. It is the visual promise upon which the entire economy of online commerce, banking, healthcare, and government services is built.

Under NNKE — theoretically — the padlock is an illusion.

> ***HTTPS = TLS + AES. TLS protects the key exchange. AES protects the session content. NNKE extracts the AES session key from the session content. TLS protection is irrelevant once the session key is extracted.***

9.1 What HTTPS Actually Protects

HTTPS encrypts the session between a browser and a server using AES. The session key is exchanged using TLS — a process now being addressed by NIST's Post-Quantum Encryption programme. But TLS protection of the key exchange is irrelevant to NNKE. NNKE does not attack the key exchange. It extracts the session key from the encrypted session traffic itself — traffic that any passive observer on the network path has always been entitled to collect.

An adversary who has collected HTTPS traffic under HNDL assumptions, and who later applies NNKE, does not need to have been present at the key exchange. They need only the ciphertext. The ciphertext was always visible. The session key was always derivable in principle. The padlock was green throughout.

9.2 What Is Exposed

Traffic Type	What Is Transmitted	Under NNKE	Who Is Affected
Banking sessions	Account numbers, balances, transfers, authentication tokens	Full session content exposed retroactively	Every online banking user
E-commerce	Payment card details, billing addresses, purchase history	Transaction intelligence extracted silently	Every online shopper
Email (webmail)	Message content, attachments, contact lists, login credentials	Years of correspondence readable	Every webmail user
Government portals	Tax returns, benefits, identity documents, official correspondence	Citizen data and government communications exposed	Every citizen using digital government
Healthcare	Medical records, diagnoses, prescriptions, insurance details	Full medical history exposed silently	Every patient using online health
Legal services	Privileged communications, case strategy, client identity	Legal privilege destroyed retroactively	Every client using online legal
Password managers	Vault unlock sequences, credential synchronisation	Every credential for every system exposed	Every password manager user
Authentication flows	MFA tokens, session cookies, OAuth exchanges	Account takeover enablement without intrusion	Every user of every web service

9.3 The Scale of Exposure

HTTPS is not a specialised protocol. It is every web interaction of any significance that has occurred in the past decade. The padlock appears on banking applications, tax portals, medical record systems, legal communications, and every form that has ever asked for a password. The scope of what has been transmitted over HTTPS under AES — and potentially stored in HNDL archives — is the sum total of human digital activity.

```
Google processes:    8.5 billion searches per day    — all HTTPS
Online banking:      Billions of sessions per day    — all HTTPS
E-commerce:          Trillions of dollars annually   — all HTTPS
Email (webmail):     Billions of messages per day    — all HTTPS
Healthcare portals:  Hundreds of millions of users   — all HTTPS
Government services: Every digital citizen           — all HTTPS

All protected by AES session keys.
All theoretically subject to NNKE session key extraction.
All stored in HNDL archives by capable state actors.
All retroactively readable if extraction succeeds.
```

9.4 The HNDL Dimension

The most devastating aspect of NNKE applied to HTTPS is not its forward-looking threat. It is the retroactive exposure of years of already-collected traffic. State actors operating HNDL programmes have stored encrypted HTTPS sessions for years under the assumption that decryption capability would eventually arrive. Under NNKE, that capability requires no quantum hardware — it requires commodity GPUs and open source frameworks.

The HNDL archive of HTTPS traffic is not a deferred liability awaiting a distant quantum future. It is a present liability awaiting a neural network engineer.

> ***The padlock was green when the traffic was collected. The padlock remains green now. The traffic is readable regardless.***

9.5 No Individual Can Protect Themselves

The individual user has no defence against NNKE applied to HTTPS. They cannot change the encryption algorithm their browser uses. They cannot choose a session key that has no geometric signature. They cannot opt out of HTTPS and use something else — there is nothing else. The protection the internet offers to individual users is AES. If AES session keys are extractable, individual users are exposed without any action or knowledge on their part.

This is not a sophisticated user problem. It is not a configuration problem. It is not a behaviour problem. It is an architectural problem that only architectural replacement can address.

10. Enterprise

The Perimeter Dissolved — The Enterprise IS HTTPS

The conventional image of enterprise security is a hardened perimeter: firewalls, intrusion detection, endpoint protection, a Security Operations Centre watching for anomalous activity. Data lives inside. Attackers are kept outside. The perimeter is the defence.

That image is obsolete. The modern enterprise has no perimeter. Over the past fifteen years, the enterprise has outsourced its entire operational infrastructure to cloud-hosted SaaS platforms, all of which communicate exclusively over HTTPS. The perimeter dissolved. The enterprise became the cloud. The cloud is HTTPS. HTTPS is AES.

> ***The sophisticated enterprise security stack — Zero Trust, SIEM, EDR, SOC — sits entirely on top of a single cryptographic primitive it has never questioned. That primitive is AES. Every tool in the stack communicates over HTTPS.***

10.1 The Outsourced Enterprise Attack Surface

The modern enterprise does not run its own systems. It subscribes to them. Every critical business function — customer management, financial operations, human resources, collaboration, identity, security — is delivered as a cloud service, accessed over HTTPS, protected by AES session keys.

Category	Platform	Data Transmitted	NNKE Consequence	Users Affected
CRM	Salesforce, HubSpot	Customer data, pipeline, contracts, strategy	Entire customer and commercial intelligence exposed	All sales & commercial staff
ERP	SAP, Oracle, NetSuite	Financial records, supply chain, operations	Full operational and financial intelligence	All operational staff
HR & Payroll	Workday, ADP, BambooHR	Salaries, personal data, performance, contracts	Every employee's personal and financial data	All employees
Collaboration	Teams, Slack, Zoom	Internal communications, meetings, decisions	Every internal conversation retroactively readable	Entire organisation
Email	Office 365, Gmail	All corporate correspondence and attachments	Years of email exposed silently	Entire organisation
DevOps	GitHub, Jira, Confluence	Source code, architecture, roadmaps, IP	Entire codebase and product strategy	All technical staff
Identity & SSO	Okta, Azure AD, Ping	Authentication flows, access tokens, user directory	Master identity infrastructure compromised	Entire organisation
Cloud KMS	AWS KMS, Azure Vault	Key management operations, master key material	Entire encryption hierarchy exposed	All encrypted systems

Security tooling	CrowdStrike, Splunk, SIEM	Security events, threat intelligence, incidents	Defender visibility turned against the defender	Security operations
Backup & DR	Veeam, AWS S3, Azure Backup	Complete data copies, recovery keys	Entire data estate retroactively accessible	All systems

The table above is not a list of optional tools. It is the operational anatomy of a typical enterprise in 2026. Remove any row and a critical business function fails. Every row communicates exclusively over HTTPS. Every HTTPS session is protected by an AES session key. Every AES session key is theoretically subject to NNKE extraction.

10.2 The Zero Trust Paradox

Zero Trust is the contemporary gold standard of enterprise security architecture. Its foundational principle: trust nothing, verify everything, assume breach. It replaces perimeter-based security with continuous authentication and authorisation at every access point.

Zero Trust is implemented over HTTPS. Its authentication flows, its token exchanges, its continuous verification signals — all transmitted over TLS and AES. An adversary applying NNKE to Zero Trust traffic does not need to defeat the Zero Trust architecture. They extract the session keys from the verification traffic itself. Zero Trust, implemented over the primitive it never questioned, provides no protection against the attack that targets that primitive.

10.3 The Security Stack Turned Against Itself

The cruelest dimension of NNKE applied to enterprise infrastructure is that the security tooling is equally exposed. SIEM platforms receiving security event data over HTTPS. Threat intelligence feeds transmitted over HTTPS. Incident response communications over HTTPS. EDR telemetry over HTTPS.

An adversary with NNKE capability applied to an enterprise's security traffic gains not just operational intelligence — they gain defender intelligence. They can read the SOC's threat assessments. They know what the organisation has detected and what it has missed. They know the incident response playbook. The security stack, transmitted over the primitive it never questioned, becomes a window into the organisation's defensive posture.

> ***The attacker who can read your security telemetry knows exactly what you can and cannot see. The defence becomes the intelligence source.***

10.4 The KMS Cascade from Enterprise Traffic

Cloud KMS operations — key generation, rotation, access grant, audit log — are transmitted over HTTPS to cloud provider APIs. An adversary applying NNKE to enterprise cloud API traffic gains session keys that decrypt KMS operational traffic. KMS operational traffic contains key material references that enable the cascade described in Chapter 3: one key extraction propagating through the entire enterprise encryption hierarchy.

The enterprise trusted its cloud KMS to protect its keys. The cloud KMS communicated over HTTPS. The HTTPS session was protected by AES. The AES session key was theoretically derivable from the traffic. The cascade was always one extraction away.

10.5 The Supply Chain Dimension

The enterprise's exposure is not limited to its own HTTPS traffic. Every SaaS vendor it uses has its own infrastructure, its own HTTPS traffic, its own AES session keys. A breach of the vendor's session keys potentially exposes all customers of that vendor simultaneously. The SolarWinds attack demonstrated the catastrophic potential of supply chain compromise through legitimate vendor access. NNKE applied to SaaS vendor traffic is the cryptographic equivalent — without the intrusion.

- Salesforce session key extracted — customer data of every Salesforce customer potentially exposed
- Okta session key extracted — identity infrastructure of every Okta customer potentially exposed
- Microsoft 365 session key extracted — email and documents of every O365 tenant potentially exposed
- AWS API session key extracted — cloud infrastructure of every AWS customer potentially exposed

The enterprise outsourced to the cloud for efficiency, resilience, and security. The cloud runs on HTTPS. HTTPS runs on AES. The outsourcing decision concentrated the attack surface into a small number of hyperscale providers whose HTTPS traffic, if subject to NNKE, exposes the global enterprise simultaneously.

11. AI Content

The End of Private AI — The Session as a Dossier

Every major AI system — ChatGPT, Claude, Gemini, Copilot, GitHub Copilot, and every API built on their foundations — communicates over HTTPS. Every prompt transmitted to an AI system. Every response received. Every document uploaded. Every conversation held. All protected by AES session keys. All theoretically subject to NNKE extraction.

But the AI threat is not merely a restatement of the HTTPS threat at one more application layer. It is categorically different in kind because of what AI sessions contain.

> ***People tell AI systems things they tell almost nobody else. Because they believe it is private. Because the padlock is green. The session is not a data point. It is a dossier. Assembled voluntarily.***

11.1 The AI Systems

AI System	Provider	Typical Session Content	NNKE Consequence
ChatGPT / GPT-4	OpenAI / Microsoft	Strategy, code, legal, medical, personal	Every prompt and response retroactively exposed
Claude	Anthropic	Analysis, documents, sensitive research, code	Every conversation and uploaded document exposed
Gemini	Google	Search-integrated queries, documents, email context	Queries plus Google account integration exposed
Copilot	Microsoft	Corporate documents, code,	Enterprise content plus AI

		O365 integration	analysis exposed
GitHub Copilot	GitHub / OpenAI	Proprietary source code, architecture	Entire codebase transmitted for completion exposed
Midjourney / DALL-E	Midjourney / OpenAI	Creative briefs, brand strategy, visual IP	Creative and brand intelligence exposed
Custom LLM APIs	Various	Fine-tuning data, RAG documents, system prompts	Proprietary AI implementation exposed
AI coding assistants	Various	Full codebase context, secrets in code	Source code, API keys, credentials exposed

11.2 What AI Sessions Actually Contain

The value of intercepted AI session content is not comparable to intercepted generic web traffic. Generic web traffic is transactional — a search query, a page view, a form submission. AI sessions are analytical. Users bring their most complex, sensitive, and confidential problems to AI systems precisely because AI can help with complexity. The session content reflects that:

- Corporate strategy — executives use AI to analyse competitive positioning, M&A targets, pricing strategy, and market entry decisions. The session contains the strategic thinking of the organisation.
- Legal analysis — lawyers and legal teams use AI to analyse contracts, assess liability, plan litigation strategy, and explore regulatory risk. Sessions contain privileged legal reasoning.
- Medical and personal — individuals use AI for medical questions they are too embarrassed to ask a doctor, personal problems they share with no one else, mental health support, and sensitive personal decisions.
- Technical architecture — engineers use AI to design systems, debug code, and explore architectural options. Sessions contain proprietary technical detail and the reasoning behind it.
- Financial planning — individuals and organisations use AI for financial modelling, investment analysis, and tax planning. Sessions contain detailed financial positions.
- Intelligence and security analysis — security researchers, government analysts, and defence personnel use AI to process and analyse sensitive information.

A single AI session from a senior government official may contain more strategically valuable intelligence than weeks of conventional traffic interception. A single AI session from a corporate executive may contain more competitive intelligence than months of email monitoring. The concentration of sensitive content in AI sessions is a function of the tool's utility — the more valuable AI is, the more sensitive the content it handles.

11.3 The Classified Network Problem

Governments have classified networks to protect sensitive discussions. Their officials then discuss strategy, policy, and intelligence assessments with AI assistants over HTTPS. The classified network was protected. The AI session was not. The padlock was green.

This is not hypothetical. AI assistant usage by government, defence, and intelligence personnel over standard HTTPS connections is documented and widespread. The convenience and capability of AI tools

has driven adoption across every sector, including those with the most sensitive information requirements. The classified network assumption — that sensitive work stays on classified infrastructure — does not survive contact with the productivity reality of AI tool adoption.

11.4 The AI Infrastructure Layer

Beyond individual sessions, AI company infrastructure presents a concentrated target of extraordinary value. The companies operating major AI systems store vast quantities of sensitive data under AES encryption:

AI Infrastructure Layer	What It Contains	NNKE Consequence
User conversation logs	Every prompt, every response, every uploaded document from every user	Entire conversation history of all users retroactively exposed
Training datasets	Proprietary and licensed data used to train models	Training data IP and licensing exposure
Model weights	The trained model — billions of parameters representing the AI's capability	Model theft — capability reproduced without training cost
Fine-tuning data	Customer-specific data used to customise models	Proprietary enterprise data submitted for fine-tuning exposed
RAG document stores	Documents uploaded for retrieval-augmented generation	Every document ever uploaded to any AI system
System prompts	Proprietary instructions defining AI behaviour and capabilities	Competitive intelligence — how AI products are built
API keys and credentials	Authentication material in developer sessions	Every API integration exposed across every customer

A successful NNKE attack against an AI provider's infrastructure KMS does not expose one user's conversation. It exposes every conversation ever held with that system, every document ever uploaded, every fine-tuning dataset every enterprise customer ever submitted. The concentration of sensitive data at AI providers — by design, as a function of the service they provide — makes them the highest-value target in the NNKE threat landscape.

11.5 The Feedback Loop

The deepest irony of NNKE applied to AI content is structural and inescapable:

```
AI is being used to:
  Analyse cybersecurity threats
  Design cryptographic defences
  Plan national security responses
  Develop post-quantum architectures
  Write research papers about NNKE and QKE
  Advise governments and organisations on
  cryptographic risk

All of that analysis:
  Transmitted over HTTPS
  Protected by AES session keys
  Stored in AI provider infrastructure
  Theoretically readable by an adversary
```

```
  with NNKE capability

The tool being used to defend against
the threat is protected by
the thing being threatened.

The defence is inside the attack surface.
```

This feedback loop is not merely ironic. It is strategically significant. An adversary with NNKE capability who targets AI session traffic gains not just intelligence about organisations — they gain intelligence about how those organisations are thinking about NNKE itself. Defensive strategies, cryptographic migration plans, vulnerability assessments, and threat analyses discussed with AI systems are all potentially readable by the adversary those discussions are designed to defend against.

11.6 The Model Theft Dimension

AI model weights represent years of training, billions of dollars of compute, and the concentrated intellectual property of the organisations that built them. They are stored encrypted under AES. A successful NNKE attack against an AI provider's infrastructure does not merely expose user conversations — it enables model theft: the extraction of the trained model itself, reproducible without the training cost, deployable in adversary infrastructure, fine-tuneable on adversary data.

The geopolitical implications of model theft at scale — the ability to reproduce frontier AI capability without the research investment — extend well beyond the cryptographic threat framework of this paper. They are noted here as a dimension of the AI infrastructure threat that has received insufficient attention in either the AI safety or the cryptographic security literature.

12. Executive Summary: The Case for Immediate Action

This document has established, on tautological grounds, that the global digital infrastructure faces a structural vulnerability of civilisational magnitude. This chapter synthesises the complete argument for those who require a single coherent statement of the threat, the consequence, and the only known resolution.

12.1 What Has Been Established

Three tautological propositions underpin this analysis. None has been disproven in the literature. None can be disproven without proof of impossibility that does not exist.

The First Tautology: The Signature Exists

> ***A key applied directly to a payload with a fixed algorithm must produce a fixed signature in the ciphertext.***

AES applies a fixed algorithm. AES applies the key directly to the payload. AES therefore produces a fixed geometric invariant in every ciphertext it generates. This is not a flaw. It is a mathematical consequence of the design. Neural networks are precisely the instrument capable of detecting geometric invariants in high-dimensional space. NNKE is therefore not merely possible — it is tautologically grounded. No proof of impossibility exists.

The Second Tautology: The Oracle Fires

> ***AES produces exactly one sensible plaintext per key. A quantum circuit in superposition across all possible keys, tested with a Selective Oracle Device, will collapse to the correct key.***

IBM Osprey reached 433 qubits in 2022. The QKE threshold is 385 qubits. The margin is 48. The hardware exists. The cost is credit-card accessible. The AI writes the circuit code. QKE is tautologically grounded. No proof of impossibility exists.

The Third Tautology: The Monoculture Amplifies Everything

> ***AES is not merely the dominant encryption standard. It is the singular encryption standard. Every system that shares a primitive shares its failure mode simultaneously.***

Banking. Finance. Military. Intelligence. Diplomatic communications. Critical infrastructure. Digital identity. Healthcare. Every HTTPS session on every device in every country. One algorithm. One point of failure. One moment of total simultaneous collapse.

12.2 What Is Already Underway

Harvest Now Decrypt Later is not a future threat. State actors are collecting and storing encrypted traffic today, under the assumption that extraction capability will mature. Under NNKE and QKE, the question is no longer when that capability arrives. The question is whether it has already arrived.

The historical record of NSA involvement in cryptographic standardisation is documented. Dual_EC_DRBG was deliberately backdoored. The BULLRUN programme explicitly targeted commercial encryption standards. The S-Box — the component performing approximately 90% of AES's cryptographic work — was parameterised during a standardisation process in which NSA participation is on record.

We make no claim about what that means. We note that the tautology exists regardless. The signature is present whether it was designed in or not.

The silence of state actors is not evidence of absence. An adversary with operational NNKE or QKE capability has every incentive to remain silent. Forensic silence is the defining property of both attacks. The correct key, producing correct plaintext, looks entirely legitimate. There is no breach to detect. There is no notification to issue. There is only the quiet reading of everything believed to be encrypted.

The question is not whether someone will attempt it. The question is not whether someone has succeeded. The question is whether they already have.

12.3 Why Post-Quantum Encryption Is Not Sufficient

NIST's Post-Quantum Encryption programme — CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+ — addresses Shor's algorithm. It protects the key exchange. It does not address NNKE. It does not address QKE. It does not address the monoculture.

A system fully compliant with NIST PQE recommendations remains fully vulnerable to key extraction from its session ciphertext. PQE reinforced the front door. NNKE and QKE enter through the window. The window is the assumption that AES ciphertext cannot be used to derive the key that produced it. That assumption is tautologically unsound.

Furthermore, PQE replaces one monoculture with another. CRYSTALS-Kyber becomes the new singular primitive. One algorithm. One point of failure. The structural vulnerability is preserved under a different name.

12.4 The Cascade: From Session Key to Total Collapse

A single AES key extraction does not expose a single dataset. It is the first domino in a trust hierarchy designed to amplify the consequence of any single failure:

- Session key extracted → all traffic for that session exposed retroactively
- KMS master key extracted → every child key, every encrypted record across the entire organisation
- TPM key extracted → entire encrypted device history across billions of devices
- Password vault key extracted → every credential, every system, entire digital identity
- CA certificate key extracted → ability to forge certificates, invisible man-in-the-middle against any trusting system

Each layer was designed to contain breach. Under monoculture conditions, each layer becomes a cascade amplifier. The architecture of trust becomes the mechanism of total exposure. Silently. With no forensic trace. With no breach notification. With no crime scene.

This is the categorical distinction between a conventional breach and Cryptographic Armageddon. A conventional breach is proportional — it damages what it touches. Cryptographic Armageddon is total — it collapses the trust infrastructure that everything else depends on. Not some systems. All systems. Not some data. All data. Not some trust. All trust.

12.5 Why Recovery Is Not Possible

A conventional breach is recoverable. Patch the vulnerability. Rotate the credentials. Notify the affected parties.

Cryptographic Armageddon is not recoverable in any conventional sense. There is no patch for a tautology. There is no credential rotation that addresses retroactive HNDL decryption. There is no breach notification because there is no breach — the key was derived, not stolen. HNDL archives already collected cannot be un-collected. Traffic already observed cannot be un-observed.

Recovery requires replacing the global cryptographic infrastructure. Every system. Every protocol. Every compliance framework. Every hardware module. Simultaneously and globally. This is not a response plan. It is a civilisational undertaking that becomes necessary the moment the extraction capability is confirmed. The time to act is before confirmation arrives. After confirmation, it is already too late.

12.6 The Only Known Solution

FES Silos is the only known architecture that addresses both the fundamental cryptographic vulnerability and the monoculture amplifier simultaneously.

FES eliminates the property that makes AES vulnerable to NNKE and QKE: the fixed transformation per key. The user-supplied password identifies a fractal transformation portal and is discarded. The payload is transformed by a non-enumerable hyperchaotic fractal stream derived from N-dimensional Mandelbrot navigation. The key never acts directly on the payload. There is no fixed geometric invariant for NNKE to detect. There is no unique plaintext for QKE's oracle to discriminate.

FES Silos eliminates the monoculture. Each Silo is a standalone cryptographic domain derived from 131,072 GUID-based reference fractal vectors. No two Silos share coordinate space. No compromise in one Silo has any mathematical relationship to any other. One Silo compromise produces isolated chaos — not a cascade.

FES achieves Shannon's perfect secrecy condition practically. The Fractal OTP satisfies the requirement that a key is used only once. Every parameter combination yields a sensible-looking plaintext from the same ciphertext — the correctness oracle cannot fire. HNDL archives of FES-encrypted traffic yield nothing. The retroactive liability does not exist.

FES is not an incremental improvement to the existing cryptographic architecture. It is a replacement of the foundation. Not better AES. Not post-quantum AES. A different thing entirely — logically impenetrable by design, unlimited in configuration, and already production-ready.

12.7 The Prevention Imperative

The asymmetry between the cost of prevention and the cost of response defines the case for immediate action.

- Prevention requires adopting post-monoculture cryptographic architecture before exploitation.
- Response — if possible at all — requires rebuilding global digital infrastructure after the fact.

The tautological foundation of this analysis is not theoretical speculation. It is mathematical necessity. The signature exists. The oracle fires. The monoculture amplifies. These are not predictions. They are logical consequences of properties AES was designed to have.

The Australian Signals Directorate and Australian Cyber Security Centre were formally notified in January and February 2026. The National Security Agency was formally notified in January 2026. The notification

was made in the spirit of discovery — not advocacy. The technology exists. It is available. A no-cost trial framework is accessible.

The question before every organisation that depends on AES — which is every organisation that operates digitally — is the same question this analysis has posed from its opening paragraph:

> **The time to address a single point of catastrophic failure is before it fails. Not after.**

12.8 What This Paper Has Not Claimed

Precision demands that the boundary of the claims in this paper be stated explicitly.

- We do not claim NNKE is operational. We assert it is theoretically possible, tautologically grounded, and that no proof of impossibility exists.
- We do not claim QKE has been executed against a live target. We assert the hardware threshold has been crossed and the tautological pathway exists.
- We do not claim the AES S-Box was deliberately backdoored. We note that the documented history of NSA involvement in cryptographic standardisation makes the question legitimate, and that the tautology holds regardless of the answer.
- We do not claim Cryptographic Armageddon has occurred. We assert that its preconditions exist, its mechanism is understood, and its consequences — once triggered — are not recoverable.

The purpose of this analysis is precisely to prevent these consequences from becoming real. A threat that is theoretically possible, tautologically grounded, and unaddressed by any current standard demands consequence analysis now — before operational confirmation arrives. By then, it is too late.

FES Silos is available for immediate evaluation at https://portalz.solutions/FES-Framework.html

The question is not whether this can happen.
The tautology established that it must be possible.
The question is whether it already has.

Acknowledgements

The AES monoculture risk framework and the Cryptographic Trust Collapse cascade model were developed by Wolfgang Flatow, drawing on six years of cryptographic architecture research and formal notifications to the Australian Signals Directorate and Australian Cyber Security Centre (January and February 2026). The consequence analysis, sector risk framework, and integration with the NNKE and QKE tautological foundations were developed through collaborative analysis with Claude (Anthropic AI System), March 2026.

References

[1] Flatow, W. (2026). Neural Net Key Extraction (NNKE). A tautological argument that AES ciphertext necessarily contains Neural Net detectable signatures. PORTALZ PTY LTD.

[2] Flatow, W. (2026). Quantum Key Extraction (QKE). A Tautological Argument for AES Quantum Vulnerability Beyond the Grover Framework. PORTALZ PTY LTD.

[3] Flatow, W. (2026). AES Key Extraction — An NIST Blind Spot. PORTALZ PTY LTD.

[4] Flatow, W. (2026). FES Peer Review Guide. PORTALZ PTY LTD.

[5] Flatow, W. (2026). Letter to Australian Signals Directorate / ACSC re: AES-256 Monoculture Risk and AIR6500. PORTALZ PTY LTD, 28 February 2026.

[6] Flatow, W. (2024). Flatow AE Algorithm — 128 Qubit AES Attack. PORTALZ PTY LTD.

[7] NIST FIPS PUB 197 (2001). Advanced Encryption Standard.

[8] NIST (2022). Post-Quantum Cryptography Standardisation. NIST IR 8413.

[9] Claude (Anthropic AI System) (2026). Independent Technical Peer Review — Fractal Encryption Standard. portalz.solutions.

[10] IBM Research (2022). IBM Osprey: 433-Qubit Quantum Processor.

[11] Shannon, C.E. (1949). Communication Theory of Secrecy Systems. Bell System Technical Journal.