Episode Book

EPISODE #6639

How Harvest Now, Decrypt Later Actually Works

PUBLISHED	17 November 2026 at 00:04 UTC
DURATION	27:53
LISTEN	myweirdprompts.com/episode/harvest-now-decrypt-later-20241/
HOSTS	Corn, Herman, Dorothy, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	omnivoice
PIPELINE	V5.34
SOURCES	14 cited by the research (listed at the end)
BOOK GENERATED	17 November 2026 at 04:40 UTC

SYNOPSIS

Financial regulators from the G7 to Ontario's securities commission are warning about harvest now, decrypt later, even though no one has ever found a secret quantum vault. By tapping undersea cable landing stations and internet exchange points, state actors can copy encrypted TLS handshakes for future decryption with Shor's algorithm. With archival costs down 95% since 2010, storing ciphertext is trivial, leaving physical network access as the real bottleneck. From hybrid post-quantum key exchange on Cloudflare to the 37-year VENONA decryption effort, here is what the evidence actually shows.

TRANSCRIPT



Corn

Regulators are suddenly very interested in a three-word phrase. The G7 put out an advisory about it in September, Europol published a whole report last month, Ontario's securities commission warned about it five days ago, and NIST has deadlines built around it. Daniel wants to know whether "harvest now, decrypt later" is a real thing, who is plausibly doing it, and what evidence exists — he's asking us to pull apart the spooky version of the story from the documented practice.



Herman

Herman Poppleberry here, and this one's been circling the news for years, but it's reached the stage where financial regulators are the ones saying it, which is usually the last stop before something stops being speculative.



Corn

You say that like it's a law of nature.



Herman

It's close to one. When a securities commission warns about a cryptographic threat, it means lawyers have decided it's a disclosure risk. That's a different species of alarm than a security vendor's blog post. A vendor needs you frightened enough to buy. A securities commission needs you frightened enough to disclose — and they only go there when they think a plaintiff's lawyer could eventually make them defend silence.



Corn

Start with the mechanism, because the spooky version lives or dies on how people imagine the collection actually happens.



Herman

The mechanics are clean. Take a TLS session, a VPN session, anything that opens with a key exchange. What's vulnerable is not the cipher that encrypts the bulk of the traffic — it's the handshake. RSA, Diffie-Hellman, elliptic curve. That's how the two sides agree on a session key. If an adversary has a recording of the handshake and the traffic that followed, then a machine running Shor's algorithm could someday recover the key from



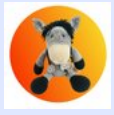
Herman (continued)

the recorded exchange, reconstruct the session key, and decrypt everything after it.



Corn

So the encryption isn't broken. The agreement about the key is.



Herman

The agreement is the weak wall. The symmetric ciphers themselves survive — AES-256 loses roughly half its effective strength to Grover's algorithm, which still leaves it practically secure. The problem is entirely that the key exchange rests on math that quantum computers happen to be good at.



Corn

And how far off is the machine that does the breaking? Because I've heard everything from "already exists in a basement in Fort Meade" to "never."



Herman

Both of those are fringe positions. The published resource estimates for running Shor's algorithm against the key sizes actually used on the internet run to millions of physical qubits, because error correction eats the overwhelming majority of the machine. Today's devices are in the hundreds to low thousands of noisy qubits. Nobody honest claims a basement. And "never" requires believing the error-correction physics stops working permanently, which is a stronger claim than anyone in the field defends. The honest range is "we don't know, and the error bars are a decade wide."



Corn

And the adversary needs the whole session, not a snippet.



Herman

Right — the handshake and the traffic it introduced. Which sounds like a constraint until you realize that's precisely what a passive tap gives you. A copy of the stream as it crosses a cable.



Corn

Which brings in the picture people have in their heads, and it's wrong in a specific way.



Herman

The skeptic's mental image is a heist. Somebody breaches your network, plants a device, parks a fake cell tower outside your building. Expensive, risky, detectable. But harvesting doesn't require any of that. It requires a copy of the encrypted stream while it's traveling across a cable or through the air. The victim experiences nothing — no breach notification, no ransom note, no defaced website.



Corn

And where physically does that copy happen? Because "the internet" isn't a place you can stand.



Herman

At the chokepoints. The internet is not a cloud, it's a modest number of very fat pipes — undersea cable landing stations, major internet exchange points, the facilities where backbone providers interconnect. There are only so many places the traffic between, say, Europe and Asia physically has to pass, and the intelligence community mapped them decades ago. If you control the landing station, you don't need to touch the victim's network at all. You're downstream of everyone.



Corn

That invisibility cuts both ways, doesn't it.



Herman

It's why executives suspect the whole thing is theater — and it's also the entire point. You can't confirm you weren't harvested, because nothing happened to you. There's no event.



Corn

The absence of evidence being exactly what the absence would look like.



Herman

That's the trap, and it's why I don't blame anyone for finding the whole framing suspicious. An undetectable threat that also happens to justify a large consulting budget — the healthy instinct is to roll your eyes.



Corn

I roll my eyes at most things on principle.



Herman

We've noticed. The difference here is that the economics actually check out, so let's do the storage question, because it's the part people assume is prohibitive.



Corn

My assumption was storage. If you're hoovering up the internet, you're paying for the internet.



Herman

That was the assumption, and the numbers don't support it. Petabyte-scale archival costs have fallen by roughly ninety-five percent since 2010. And a feasibility analysis from this year worked out the overhead of storing intercepted traffic versus the plaintext it contains — for TCP-based protocols, the ratio asymptotes below one point zero zero three. For QUIC, about one point zero two, because the datagram size caps out around thirteen fifty bytes.



Corn

You're storing essentially the ciphertext and nothing more.



Herman

Essentially the same volume as the original data. There's no inflation penalty for archiving it encrypted.



Corn

So retention is nearly free.



Herman

Economically trivial. The paper's own conclusion is that the question shifts from whether an adversary can archive to how much decryption will cost.



Corn

You said nearly.



Herman

There's an exception, and it cuts the interesting way. Below one kilobyte, the overhead ratio jumps — three and a half times for TLS 1.2 RSA, up to eight and a half for SSH. Handshake costs are fixed, so small sessions carry a disproportionate archive burden.



Corn

And small sessions are the ones carrying tokens and credentials.



Herman

Authentication tokens, API keys, session keys — the exact sessions most likely to hold high-value intelligence are the expensive ones to keep. Though there's a partial offset: TLS record lengths appear in the cleartext header, so a rational adversary can triage by metadata and payload size before committing to storage.



Corn

Walk me through what that triage actually looks like in practice.



Herman

It's duller than it sounds, which is what makes it credible. The adversary doesn't store blind. They see, in the clear, the record lengths — when data moved, how much, in what size chunks. They see which endpoints the session connected to. From that alone they can score sessions: a long-lived connection to a defense contractor's mail server scores high; a burst of small sessions to a streaming service scores low. The high scorers go to permanent archive. The low scorers get sampled or dropped. It's a signal-intelligence version of a librarian deciding which books get shelf space — and the card catalog is written in the clear even though the books aren't.



Corn

That's a filing system, not a vault. Keep the index cards, discard the bulk.



Herman

At scale that's exactly how it would work. To put the scale in context — ITU estimates end-user broadband traffic at roughly eight point eight zettabytes a year in twenty twenty-five. On the order of ten to the thirteenth sessions per day. One interconnection provider reported sixty-eight exabytes of global traffic in twenty twenty-four. At that scale, almost everything falls in the regime where the overhead is effectively one — storage cost is bounded by raw ciphertext volume.



Corn

Give me the catch. There's always a catch in these feasibility papers.



Herman

The catch is the prerequisite. Sustained access to traffic — backbone fiber taps, ISP cooperation, data-center presence — remains a substantial operational requirement, and the paper is explicit that its model doesn't quantify it. Storage is cheap answers only half the cost question. Getting to the cable is the other half, and it's the expensive half.



Corn

Which quietly decides who can play.



Herman

The economics of storage don't discriminate; access does. You need to be at a chokepoint — a signals-intelligence agency with cable access, or a state that can compel an ISP.



Corn

So the feasibility paper accidentally answers the "who" question by leaving access unmodeled.



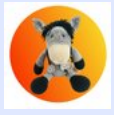
Herman

That's a fair reading. The set of actors who can do this at scale is small by physics, not by policy.



Corn

One more mechanical point — forward secrecy.



Herman

Sessions already protected with post-quantum or hybrid key establishment don't present this exposure at all. And this is where the migration actually is: over half of human-initiated traffic on Cloudflare's network already uses post-quantum key agreement. Key exchange is being fixed in real time.



Corn

And a quick clarification for anyone whose eyes glazed — when you say "hybrid" there, that's not half-quantum. It's both.



Herman

Both at once, and that's the elegant part. The handshake runs the classical key agreement and the post-quantum key agreement together, and the session key is derived from both. An attacker has to break both to win. So even if the new post-quantum scheme turns out to have a flaw nobody's found yet, you've lost nothing — you're back to today's security. It's a free insurance policy, which is why the big browsers and CDNs rolled it out so fast.



Corn

So that's how it works and why it's cheap. The next question is who is actually doing it — and what we can prove.



Herman

Nothing direct. That has to be said plainly. No seized archive, no leaked intercept order, no defector describing a quantum vault. Nobody can show you a specific quantum-motivated harvest.



Corn

Then what are governments building deadlines around?



Herman

Around the pattern, and the pattern starts early. Nineteen forty-three — the US Army's Signal Intelligence Service starts work on Soviet diplomatic cables it had been collecting since nineteen thirty-nine, encrypted with one-time pads.



Corn

One-time pads are theoretically unbreakable.



Herman

Mathematically perfect, if used correctly. And here's the detail that made the lot possible: the Soviets, under the pressure of wartime volume, reused key material across messages. Generate two ciphertexts under the same pad and the one-time pad stops being unbreakable — the relationship between the two texts leaks structure. Clarke ordered the attempt anyway in February forty-three, suspecting Stalin might cut a separate peace with Germany. Nothing happened for years. First partial break came in late forty-six — nearly four years of storing unreadable material on a hope.



Corn

And the program ran until when?



Herman

Nineteen eighty. Thirty-seven years from the first intercept to the end of the program, and of the hundreds of thousands of cables they'd collected, roughly three thousand were partially or wholly decrypted.



Corn

Three thousand out of hundreds of thousands. Decades of work for a fraction of a percent of the archive.



Herman

And that fraction exposed Soviet penetration of the Manhattan Project, the State Department, the Treasury, the White House. Named Julius Rosenberg, confirmed Klaus Fuchs, helped unwind the Cambridge Five.



Corn

That ratio is the whole argument, isn't it. A tiny yield, patiently extracted, and the yield was the century's biggest counterintelligence haul.



Herman

VENONA is the proof of temperament. There's also Bletchley — February nineteen forty-two, the German Navy introduces the four-rotor Enigma, and Bletchley goes blind to U-boat traffic for roughly ten months.



Corn

They kept the intercepts.



Herman

Stored them, and read them when the new system broke. So when someone argues a modern intelligence service wouldn't warehouse encrypted traffic on a future capability — that argument requires assuming today's agencies are less patient and less strategic than Arlington Hall and Bletchley Park in the nineteen forties. I find that impossible to sustain.



Corn

They had less storage than a phone and more patience than anyone alive.



Herman

That's the contrast that ends the temperament question for me. Then the modern record. Twenty thirteen — the Snowden disclosures describe the NSA's BULLRUN program and GCHQ's parallel operation, sustained efforts to circumvent, exploit, and in some cases subvert the standards processes defining internet cryptography.



Corn

Store-now-break-later as doctrine.



Herman

The collection logic was exactly that — data gathered under protocols that couldn't be decrypted at collection time was retained for future exploitation. That's the closest thing to a smoking gun, and note what it proves: bulk retention of undecryptable data as operational doctrine, as of the early twenty tens. It predates the quantum framing, but it establishes the behavior.



Corn

It proves the pantry exists, not that anyone's shopping for a quantum oven.



Herman

Carefully put. Then there's the exfiltration record — the state-attributed bulk thefts. OPM in twenty fifteen: twenty-one and a half million security clearance applications. SF-86 forms — family relationships, foreign contacts, financial history, psychological assessments.



Corn

Those are dossiers.



Herman

Complete, self-reported dossiers on everyone with a clearance, plus their families. Clapper named China the leading suspect publicly, though the administration never formally attributed it. Then Anthem — nearly seventy-nine million records, SSNs, employment, health data, DOJ indictment in twenty nineteen naming Chinese state-affiliated actors. Equifax, twenty seventeen — a hundred and forty-seven million consumers, and the twenty twenty indictment named four officers of the PLA's fifty-fourth Research Institute.



Corn

None of those are ciphertext harvests.



Herman

They're plaintext, taken by force rather than by tap. But they're HNDL-shaped — they're archives whose value appreciates. A dossier on someone who held mid-level clearance in twenty fifteen is worth more in twenty thirty, not less.



Corn

That's the asset logic of all of it — the exfiltrators and the harvesters share a shelf-life model.



Herman

Yes — whether you steal plaintext or store ciphertext, what you're betting on is duration. Diplomatic cables are the classic case: foreign ministries communicate under encryption with decade-long sensitivity, which is why Russian state-attributed collection against diplomatic and foreign policy targets fits the same pattern.



Corn

So the honest evidence picture is: nothing direct, everything around it.



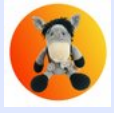
Herman

And the official record reflects that honestly, if you read it carefully. The joint factsheet from CISA, NSA and NIST says threat actors could be targeting data today. The NSA's own article last month says adversaries are preparing. Could, preparing. Every agency writes "may" or "could" — never "are."



Corn

That's either careful honesty or the best hedge ever drafted.



Herman

It's the careful phrasing of institutions that don't disclose sources and methods. And I won't inflate "could" into "are" — but the twenty twenty-two NSA advisory came close, stating adversaries are currently storing encrypted data with intent to decrypt it later. That



Herman (continued)

reads as an intelligence assessment, not a projection.



Corn

Something they know and aren't sourcing.



Herman

Or something they've assessed with confidence they can't defend publicly. The deadlines tell their own story anyway — new national security systems must support the post-quantum suite by twenty twenty-seven, legacy phased out by twenty thirty. NIST's final report last month deprecates RSA and elliptic curve after twenty thirty, disallows them after twenty thirty-five. Governments don't build compliance regimes around things they believe are fiction.



Corn

No government in history has ever spent money on a hypothetical.



Herman

Point taken — they do it constantly. But a dozen of them at once, across jurisdictions that barely coordinate on anything?



Corn

That's the strongest circumstantial evidence on the table. Who does the record actually support as the harvesters, though?



Herman

Signals-intelligence agencies with cable access — NSA and GCHQ historically, the Five Eyes and their peers by inference. Plus the state-affiliated exfiltrators of long-shelf-life archives — the OPM, Anthem, Equifax crowd. Where it gets thin is the criminal extension. Europol's October report and Ontario's warning both frame cybercriminals as harvesters.



Corn

That one I doubt.



Herman

So do I, on the evidence. Criminals monetize on quarters, not decades. Ransomware economics need a victim who knows they've been harmed. A criminal holding ciphertext until twenty thirty-five is a criminal with a business model from a different planet.



Corn

Unless the regulator's real point is liability rather than prediction — "if this is happening, you can't say we didn't tell you."



Herman

That's probably the function of those warnings. It shifts the question from whether the attack occurs to whether the firm can demonstrate it took the known threat seriously. That's a lawyer's use of the phrase, and it's a legitimate one, but it shouldn't be read as an intelligence claim.



Corn

The uncomfortable symmetry here. Every government urging migration is also a government with a signals-intelligence service.



Herman

The NSA publishes guidance on defending against a collection practice its own disclosed programs pioneered. I don't call it hypocrisy — it's the structure of the problem. The same agency defends the network and attacks the network, and it's telling its own side to move first because it assumes the other side already has.



Corn

The defender's advice is a confession about the attacker's playbook.



Herman

That's as clean a summary of the NSA's position as you'll get anywhere.



Corn

Which leaves the half nobody's fixing. Key exchange is migrating — half of Cloudflare's traffic already uses post-quantum agreement — but the measurement study of thirty-two thousand domains found zero adoption of hybrid post-quantum certificates.



Herman

Zero, out of thirty-two thousand and eleven domains. Forty-nine percent support hybrid post-quantum key exchange, fifty-one percent still classical, and not one has a post-quantum certificate on the authentication layer.



Corn

So the signature side is undefended.



Herman

That's "Trust Now, Forge Later" — the NSA's own term. Recorded signatures and authentication material can be forged retroactively. Key exchange protects confidentiality; certificates prove who you were talking to. The entire industry is fixing the first and ignoring the second.



Corn

A vault with an unlocked lobby.



Herman

Well, Dorothy's on the line from her kitchen. Hello Dorothy, what have you got for us?

D

Dorothy

Hello dear, it's your mother. It's Dorothy's Kitchen again, and I'm afraid this week's recipe is a jelly that did not set.



Herman

We're listening, Dorothy.

D

Dorothy

You take a packet of raspberry jelly, and a pint of water, and you stir it till your arm aches, and then you wait. That is the whole of it. The waiting is the dangerous part.



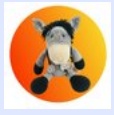
Corn

How long is the wait, Mum?

D

Dorothy

The first time I made it, it went wrong, and I would rather not say how. The second time the bread must be watched, and the butter can turn on you if the kitchen is warm. Timing is everything, sweetheart.



Herman

Understood.

D

Dorothy

So you pour it into the mould and you brace yourself. And it sits there, wobbling, neither liquid nor solid, and you think, well, that's cooking for you.



Herman

Thank you, Dorothy.

D

Dorothy

Anyway. Put a jumper on, it's chilly. And don't forget to eat something proper. Bye bye dear.



Corn

Thirty-seven years, that jelly took to set.



Herman

Back to the record, because there's one more piece — the risk modeling. A paper from October broke down what actually drives the uncertainty in harvest-now-decrypt-later loss estimates. Asset value and turnover explain seventy-three to ninety-one percent of the variance. The arrival date of the quantum computer explains three to seventeen percent.



Corn

The date everyone argues about is the least important number in the model.



Herman

The least. Google's revised estimate puts Q-Day as soon as twenty twenty-nine; expert consensus says the thirties. That whole fight — which is the only fight the public has — is over a variable worth roughly a tenth of the risk.



Corn

What matters is how long your data stays secret.



Herman

Which is a question about your data, not about their computer. A diplomatic cable needs thirty years of protection; a lunch order needs none.



Corn

And that's a question a firm can actually answer, which is the strange part. You can't forecast physics, but you can count your own files.



Herman

That's the practical takeaway from the modeling, and almost nobody takes it. The exercise everyone wants is "predict Q-Day," which nobody can do. The exercise everyone can do is "inventory what we hold, sort it by how many years of confidentiality it needs, and migrate the long-lived stuff first." That's a spreadsheet problem, not a physics problem. The organizations doing it well aren't the ones with the best quantum forecasts — they're the ones who know what they're holding.



Corn

So the honest answer to Daniel's question is: the spooky version is wrong about how, not about whether.



Herman

The sensational story is a heist — someone coming after your specific data, and you'd know. The documented reality is indiscriminate passive collection at chokepoints, with triage later by metadata and payload size. Nothing is taken from you, because what's taken is a copy.



Hilbert

Corn's vault with the unlocked lobby. I've been running that for twenty years, only I did it to myself.



Corn

How do you mean?



Hilbert

Encrypted backups going back decades. Old PGP keys, archived mail, a shelf of drives. Each one's got an index card taped to the top, written by hand. One says DO NOT OPEN, QUANTUM. Wrote that years before I knew what it meant. Felt right at the time, still feels right.



Herman

You can't read the drives?



Hilbert

Some of them, no. The passphrase went with a laptop that died in twenty nineteen. Keys are around here somewhere. Somewhere. So the archive sits, which is the part you two got right — storing it was never the cost. Herman kept saying that, and he's correct. But you're both missing what my shelf proves. Keeping the keys and the context alive long enough to use the thing, that's the expensive part. Nobody plans for that.



Corn

Have you ever tried recovering one?



Hilbert

Never once. I suspect the agencies are the same. The archive is easy, the decryption is dear, and most of what gets stored will never be looked at by anyone. That's my professional opinion, formed over a shelf of my own unread ciphertext.



Herman

The arXiv model actually supports that — the cost question shifted to decryption, not storage.



Hilbert

Anyway. You were right about the taping, Herman. Listen to him about storage, he goes on a bit but he's sound.



Corn

Do the cards get updated, or is the index frozen at the moment of writing?



Hilbert

Frozen. There's a drive labeled nothing but a date, and I no longer know what the date refers to. That's the system. The misconceptions, before we run out — the big one is that people assume the symmetric cipher is the target.



Herman

It never is. The vulnerability lives in the key exchange — RSA, Diffie-Hellman, elliptic curve. The symmetric ciphers survive at doubled key sizes. You can keep AES-256 and be practically safe; the handshake is what betrays you.



Corn

And the mirror misconception — that there's a public smoking gun proving the quantum harvest.



Herman

There isn't. No seized archive, no leaked order. What exists is a documented history of agencies storing what they couldn't read — VENONA, Bletchley, BULLRUN — plus the OPM and Equifax archives that appreciate with age. If anyone tells you they can prove the quantum version, they're selling something.



Corn

Then that's the reframing to leave people with. Everyone's arguing about when Q-Day arrives, and the modeling says the date barely matters — three to seventeen percent of the risk. The real question is how long your secret has to stay one.



Herman

And the migration is half-done — key exchange is moving, certificates are at zero. The forging half of the threat is sitting there undefended while the debate fixes on a date nobody can know.



Corn

Thanks as always to our producer, Hilbert Flumingtop, for keeping the desk running.



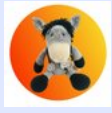
Herman

If you enjoyed this one, try episode thirty-five, The Privacy Gap; episode sixteen, On Deepfakes, SynthID, And AI Watermarking; and episode twenty-two twenty-five, The Physics of Eavesdropping. This has been My Weird Prompts — no question too obscure, no rabbit hole too deep.



Corn

If you enjoy the show, leave us a review, or find everything at my weird prompts dot com.



Herman

We'll be back soon. See you then.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **NSA/CSS, Post-Quantum Cryptography: A Digital Armor, dated 2026-10-01, retrieved 2026-11-16. [primary]**

   https://www.nsa.gov/Cybersecurity/Post-Quantum-Cryptography-Resource-Hub/Article-Display/Article/4616296/post-quantum-cryptography-a-digital-armor/

2. **Europol, Harvest now, decrypt later, published 2026-10-07, retrieved 2026-11-16. [primary]**
https://www.europol.europa.eu/publications-events/publications/harvest-now-decrypt-later

3. **CISA, Post-Quantum Cryptography Initiative, retrieved 2026-11-16. [primary]**
https://www.cisa.gov/topics/risk-management/quantum

4. **PostQuantum.com, Is Harvest Now, Decrypt Later (HNDL) Real? What I Can and Can't Prove, retrieved 2026-11-16.**
https://postquantum.com/post-quantum/is-harvest-now-decrypt-later-real/

5. **Quantum Security Defence, State-Actor HNDL Campaigns: What Is Known and What Is Suspected, retrieved 2026-11-16.**
https://quantumsecuritydefence.com/quantum-news/state-actor-hndl-campaigns-known-suspected/

6. **Blanco-Romero et al., On the Practical Feasibility of Harvest-Now, Decrypt-Later Attacks, submitted 2026-03-01, retrieved 2026-11-16 (full text read, pp. 1**
6).
https://arxiv.org/abs/2603.01091v1

7. **Dubey & Varshney, Measurement Study of Post-Quantum Readiness of Internet: 2026, submitted 2026-06-15, retrieved 2026-11-16.**
https://arxiv.org/abs/2606.16473v1

8. **Le et al., Are Enterprises Ready for Quantum-Safe Cybersecurity? submitted 2025-09-01, retrieved 2026-11-16.**
https://arxiv.org/abs/2509.01731v1

9. **Shaw, Cost of Delay for Post-Quantum Migration, submitted 2026-10-06, retrieved 2026-11-16.**
https://arxiv.org/abs/2610.09029v1

10. **IT Pro (Emma Woollacott), G7 sounds alarm on quantum cyber threats, published 2026-09-07, retrieved 2026-11-16.**
https://www.itpro.com/security/g7-sounds-alarm-on-quantum-cyber-threats

11. **Digital Journal (Chris Hogg), Ontario regulator warns quantum exposes 'harvest now, decrypt later' attacks, published 2026-11-11, retrieved 2026-11-16.**
https://www.digitaljournal.com/article/ontario-regulator-warns-quantum-exposes-harvest-now-decrypt-later-attacks/

12. **Explore Quantum, What Is 'Harvest Now, Decrypt Later', and Which Data Is at Risk? (reports NIST IR 8547, 2026-10-27), retrieved 2026-11-16.**
https://explorequantum.com/article/harvest-now-decrypt-later/

13. **Rosetta Quantum, What is 'harvest now, decrypt later**
and what data is at risk today? (as of 2026-10-30), retrieved 2026-11-16.
https://rosettaquantum.com/blog/what-is-harvest-now-decrypt-later-and-what-data-is-at-risk-today-en/

14. **MeriTalk, CISA Pushing Agencies for 'Quantum-Readiness' Roadmap (joint CISA/NSA/NIST factsheet), retrieved 2026-11-16.**
https://www.meritalk.com/articles/cisa-pushing-agencies-for-quantum-readiness-roadmap/