Strategische Infrastrukturanalyse: HNDL-Architekturen, Netzwerküberwachung und Quantenkryptoanalyse

1. Einleitung und strategischer Kontext

Die moderne Signalaufklärung (Signals Intelligence, SIGINT) hat sich von der taktischen Echtzeitüberwachung hin zu einer langfristigen strategischen Akquise verschoben, die unter dem Paradigma „Harvest Now, Decrypt Later“ (HNDL) bekannt ist. Dieses Konzept postuliert die massenhafte Speicherung verschlüsselter Datenströme, deren kryptografischer Schutz nach aktuellem Stand der Technik (Stand 2025/2026) nicht oder nur mit unverhältnismäßigem Aufwand zu durchbrechen ist. Das Ziel dieser Strategie ist die Archivierung von Informationen, die eine langfristige Relevanz besitzen – diplomatische Kabel, militärische Entwicklungspäne, biometrische Datenbanken und strategische Industriekommunikation – um sie zu einem späteren Zeitpunkt zu entschlüsseln. Dieser Zeitpunkt, oft als „Q-Day“ bezeichnet, tritt ein, wenn entweder mathematische Durchbrüche in der Kryptoanalyse erzielt werden oder, was als wahrscheinlicher gilt, ein kryptografisch relevanter Quantencomputer (CRQC) verfügbar wird.

Dieser Bericht bietet eine erschöpfende technische Untersuchung der für HNDL notwendigen physischen und logischen Infrastruktur. Er analysiert primär das Utah Data Center der National Security Agency (NSA) als zentrales Speicherreservoir und untersucht die Rolle der globalen DNS-Infrastruktur sowie des Internet-Backbones als Akquise-Vektoren. Ein kritischer Aspekt dieser Analyse ist die Untersuchung, ob und wie diese Infrastruktur genutzt wird, um durch aktive Netzwerkangriffe (Downgrade-Attacken) die Verschlüsselungsqualität der gesammelten Daten präventiv zu schwächen. Abschließend erfolgt eine detaillierte Gegenüberstellung der Hardware-Architekturen von Quantencomputern, um den Zeithorizont für die Entschlüsselung von Standardalgorithmen wie RSA-2048 und ECC zu prognostizieren.

---

2. Das Utah Data Center: Physische Basis der HNDL-Strategie

Das Utah Data Center (UDC), offiziell bezeichnet als *Intelligence Community Comprehensive National Cybersecurity Initiative Data Center*, stellt die physische Manifestation der

HNDL-Doktrin dar. Gelegen am Camp Williams nahe Bluffdale, Utah, dient diese Anlage als primäres Archiv für die US-Intelligence Community. Die Analyse der verfügbaren technischen Daten erlaubt Rückschlüsse auf die Kapazität und die operative Ausrichtung der Anlage.[1]

2.1 Architektonische Spezifikationen und Energiebilanz

Die Anlage umfasst eine Gesamtfläche von ca. 1 bis 1,5 Millionen Quadratfuß (ca. 93.000 bis 140.000 Quadratmeter). Entscheidend für die Bewertung der technologischen Leistungsfähigkeit ist jedoch die Aufteilung dieser Fläche. Die eigentliche missionskritische Rechenzentrumsfläche (Tier III raised floor space) wird auf ca. 100.000 Quadratfuß (ca. 9.300 Quadratmeter) beziffert.[2] Der verbleibende Raum von 900.000 Quadratfuß dient der technischen Infrastruktur (Stromversorgung, Kühlung, Administration).

Der Energieverbrauch der Anlage ist ein direkter Indikator für ihre Funktion. Mit einer geschätzten Leistungsaufnahme von 65 Megawatt gehört das UDC zu den energieintensivsten Rechenzentren der Welt. Diese enorme Energieaufnahme wird benötigt, um sowohl die Serverfarmen zu betreiben als auch die massive Abwärme über Kühltürme und Chiller-Systeme abzuführen, die täglich bis zu 1,7 Millionen Gallonen Wasser verbrauchen.[2] Diese Energiebilanz deutet darauf hin, dass das UDC nicht als reines „Cold Storage" (Passivarchiv) konzipiert ist, sondern über massive Rechenkapazitäten für die Echtzeit-Datenverarbeitung (Ingest), Indexierung und Metadaten-Analyse verfügt. Die Verarbeitung von Exabytes an Daten erfordert Hochleistungs-Cluster, um Datenströme zu normalisieren und für die Langzeitspeicherung vorzubereiten.

2.2 Analyse der Speicherkapazität: Yottabyte-Mythos vs. Realität

In der öffentlichen Diskussion und frühen Berichterstattung wurden Kapazitäten im Bereich von „Yottabytes" (1 Yottabyte = 10^{24} Bytes) kolportiert.[2] Eine technisch-ökonomische Analyse widerlegt diese Größenordnung jedoch unter Berücksichtigung der physikalischen Dichte von Speichermedien und der verfügbaren Bodenfläche.

2.2.1 Festplattenspeicher (HDD) Szenario

Ein Yottabyte entspricht einer Billion Terabytes. Selbst unter der Annahme modernster Helium-gefüllter Festplatten mit hoher Speicherdichte (z.B. 20-24 TB pro Laufwerk) und einer extrem dichten Packung in Standard-Racks, würde die Speicherung eines Yottabytes Investitionen im Bereich mehrerer Billionen US-Dollar erfordern – ein Betrag, der das gesamte US-Bruttoinlandsprodukt übersteigen könnte.[3] Zudem würde der Platzbedarf für die notwendigen Racks die 100.000 Quadratfuß des UDC um ein Vielfaches überschreiten.

2.2.2 Magnetband (Tape) als HNDL-Medium

Für die HNDL-Strategie ist Magnetband (Tape) die einzig plausible Technologie.
Tape-Libraries bieten die geringsten Kosten pro Terabyte und verbrauchen im Ruhezustand

keine Energie, was für Daten, die über Jahrzehnte gelagert werden sollen („Store Now“), essenziell ist.
Kritische Analysen, unter anderem von ehemaligen NSA-Mitarbeitern wie William Binney, korrigierten die Schätzungen auf den Bereich von 5 Zettabytes (1 Zettabyte = 10^{21} Bytes).3 Doch selbst 5 Zettabytes stellen eine logistische Herausforderung dar. Eine Standard-Tape-Library (z.B. Oracle StorageTek SL8500) hat eine bestimmte physische Grundfläche. Um 5 ZB zu speichern, wären bei heutiger LTO-Technologie (Linear Tape-Open) Flächen von ca. 420.000 Quadratmetern notwendig – deutlich mehr als die verfügbare Fläche im UDC.4
Schlussfolgerung zur Kapazität:
Es ist davon auszugehen, dass die reale Kapazität des UDC im Bereich hoher Exabytes bis hin zu wenigen Zettabytes liegt. Dies ist ausreichend, um den globalen verschlüsselten Verkehr von Hochwertzielen (High-Value Targets) über Jahre hinweg zu speichern. Die „Yottabyte“-Aussagen sind als psychologische Kriegsführung oder Missverständnis technischer Präfixe zu werten. Das UDC ist modular aufgebaut, was eine stetige Verdichtung der Speichertechnologie (z.B. Migration von LTO-9 auf LTO-10+) ohne bauliche Erweiterung erlaubt.2

2.3 Tabelle: Infrastrukturelle Kenndaten UDC

Parameter	Spezifikation / Schätzung	Implikation für HNDL
Standort	Bluffdale, Utah (Camp Williams)	Schutz durch militärische Zone, Zugang zu Energie/Wasser
Gesamtfläche	~1.000.000 - 1.500.000 sq ft	Massive Infrastruktur für Support und Sicherheit
Rechenzentrumsfläche	~100.000 sq ft (Tier III)	Begrenzt die Anzahl der Racks; Fokus auf High-Density Storage
Leistungsaufnahme	~65 Megawatt	Ermöglicht massives Computing für Ingest & Kryptoanalyse
Kühlbedarf	~1,7 Mio. Gallonen Wasser/Tag	Indikator für hohe thermische Last durch aktive Server

Geschätzte Kapazität	Exabytes bis niedrige Zettabytes	Ausreichend für selektive globale Vollüberwachung
Speichermedium	Primär Tape Robots, Sekundär HDD/SSD	Tape für Langzeit-HNDL, HDD für Index/Metadaten

---

3. Überwachungsarchitektur: Root-Server und Backbone-Infrastruktur

Die HNDL-Strategie erfordert Zugriff auf Datenströme. Die Analyse der Netzwerk-Topologie zeigt, dass die öffentliche Fokussierung auf die DNS Root-Server oft von den tatsächlich kritischen Überwachungspunkten im Internet-Backbone ablenkt.

3.1 Die Rolle der 13 Root-Server: Mythos und Limitierung

Das Domain Name System (DNS) wird oft als das „Telefonbuch" des Internets bezeichnet. An der Spitze der Hierarchie stehen die Root-Server, die technisch durch 13 IP-Adressen (Identitäten A bis M) repräsentiert werden.
Es ist ein weit verbreiteter Irrtum, dass die Überwachung dieser 13 Server eine Kontrolle über das Internet oder Zugriff auf Inhalte ermöglicht.5

1. **Anycast-Architektur:** Die 13 logischen Server entsprechen nicht 13 physischen Maschinen. Durch Anycast-Routing werden diese IP-Adressen von tausenden Servern an hunderten Standorten weltweit propagiert.[5] Eine physische Kompromittierung aller Knoten ist unmöglich.
2. **Dateninhalt:** Root-Server beantworten Anfragen für Top-Level-Domains (TLD) wie .com oder .org. Sie sehen in der Regel nur die IP-Adresse des anfragenden DNS-Resolvers (z.B. eines ISP oder Google Public DNS) und die angefragte TLD. Sie sehen *keine* URLs, *keine* Pfade und *keine* Nutzerdaten.[7]
3. **Fehlkonfigurationen als Datenquelle:** Analysen haben gezeigt, dass bis zu 98% des Verkehrs an Root-Servern „Müll" ist – verursacht durch falsch konfigurierte Firewalls oder interne Netzwerkanfragen, die fälschlicherweise ins öffentliche Netz lecken.[8] Dies bietet zwar Einblicke in interne Netzstrukturen, ist aber für HNDL von verschlüsselten Inhalten irrelevant.

3.2 Das reale Ziel: Backbone-Interception („Upstream")

Die NSA-Programme, die unter dem Begriff „Upstream" zusammengefasst werden (u.a. STORMBREW, FAIRVIEW, BLARNEY), zielen nicht auf die Endpunkte, sondern auf die Transportwege.[9] Die Überwachung findet direkt an den Glasfaserkabeln und Core-Routern

der großen Tier-1-Provider und Telekommunikationsunternehmen statt.[10]

3.2.1 Physische Interception-Techniken

Die Dokumente von Edward Snowden und Enthüllungen über Räume wie „Room 641A“ in San Francisco belegen den Einsatz von optischen Splittern (Beam Splitters). Diese passiven Geräte werden in die Glasfaserleitungen eingeschleift und leiten einen Teil des Lichtsignals (z.B. 10-30%) an die Überwachungsgeräte ab, während das Hauptsignal ungestört weiterfließt.[10] Da dies auf Layer 1 (Physical Layer) geschieht, ist es für Sender und Empfänger technisch nicht detektierbar.

3.2.2 Router-Implantate und Supply Chain Interdiction

Zusätzlich zur physischen Anzapfung hat die NSA, spezifisch die Abteilung Tailored Access Operations (TAO), Firmware-Modifikationen für Router großer Hersteller (Cisco, Juniper, Huawei) entwickelt.[11] Diese Implantate ermöglichen es, Datenpakete nicht nur zu kopieren, sondern auch Routing-Entscheidungen zu manipulieren oder Pakete gezielt umzuleiten. Berichte zeigen, dass US-Behörden Hardware auf dem Transportweg abfingen, manipulierten und neu verpackten, bevor sie an Zielkunden (oft ausländische Telcos) ausgeliefert wurde.[11]

3.2.3 BGP-Hijacking und Routing-Anomalien

Das Border Gateway Protocol (BGP), das Routing-Rückgrat des Internets, basiert weitgehend auf Vertrauen. Angriffe auf BGP, wie das Hijacking von Root-DNS-Präfixen, ermöglichen es Akteuren, den Verkehr ganzer Regionen über eigene Überwachungsknoten umzuleiten.[13] Cisco ThousandEyes und andere Monitoring-Dienste haben solche Anomalien dokumentiert. Für HNDL ist dies wertvoll, da so Verkehr, der normalerweise nicht durch US-Hoheitsgebiet fließen würde, künstlich über US-Knoten (und damit NSA-Sensoren) geleitet werden kann.[14]

---

4. Analyse aktiver Downgrade-Attacken

Eine zentrale Fragestellung ist, ob die Infrastruktur lediglich passiv sammelt oder aktiv eingreift, um die Qualität der Verschlüsselung zu reduzieren („Downgrade“). Die Beweislage deutet stark auf Letzteres hin: Um die Zeit bis zur Entschlüsselung („Decrypt Later“) zu verkürzen, wird versucht, die Verschlüsselungsstärke bereits zum Zeitpunkt der Ernte („Harvest Now“) zu minimieren.

4.1 Das QUANTUM-Programm: Man-on-the-Side Mechanismen

Das NSA-Programm QUANTUM (insbesondere QUANTUMINSERT) nutzt die privilegierte Position im Backbone für sogenannte „Man-on-the-Side“ (MotS) Angriffe. Anders als ein Man-in-the-Middle (MitM), der den Datenstrom blockieren kann, liest der MotS nur mit, kann

aber eigene Pakete injizieren.[15]

Technischer Ablauf eines QUANTUM-Angriffs:

1. **Detektion (TURMOIL):** Sensoren im Backbone erkennen eine Ziel-Verbindung (z.B. einen TCP-Handshake oder HTTP-Request eines überwachten Ziels).
2. **Trigger:** Das System alarmiert einen Shooter-Server (Codename FOXACID).
3. **Race Condition:** Der FOXACID-Server sendet ein gefälschtes Antwortpaket an das Opfer, das so konzipiert ist, dass es *vor* der legitimen Antwort des echten Servers eintrifft. Da die NSA-Server oft strategisch besser im Backbone platziert sind (geringere Latenz), gewinnt das NSA-Paket das „Rennen".[16]
4. **Übernahme:** Der Browser des Opfers akzeptiert das gefälschte Paket (da IP, Port und TCP-Sequenznummern korrekt vorhergesagt/gelesen wurden) und verwirft das spätere echte Paket als Duplikat.

4.2 Begünstigung von Protokoll-Downgrades

Diese MotS-Fähigkeit wird genutzt, um Verschlüsselungsprotokolle anzugreifen.

4.2.1 TLS Stripping und Version Rollback

Obwohl moderne Browser und Server versuchen, die stärkste Verschlüsselung (z.B. TLS 1.3) auszuhandeln, existieren Mechanismen zur Abwärtskompatibilität. Ein aktiver Angreifer kann in den ClientHello-Handshake eingreifen und simulieren, dass Verbindungsfehler auftreten, wenn höhere Protokollversionen genutzt werden. Dies zwingt viele Clients (insbesondere ältere IoT-Geräte oder Legacy-Browser) dazu, einen Fallback auf unsichere Protokolle wie SSL 3.0 durchzuführen.18
Der POODLE-Angriff (Padding Oracle on Downgraded Legacy Encryption) basiert exakt auf diesem Prinzip: Der Angreifer erzwingt einen Downgrade auf SSL 3.0 und nutzt dann dessen Schwächen im Padding, um Inhalte zu entschlüsseln.19

4.2.2 Kryptografische Downgrades: Logjam und FREAK

Besonders relevant für HNDL sind Angriffe auf den Schlüsselaustausch.

- **Logjam (Diffie-Hellman):** Viele Server unterstützten lange Zeit noch „Export-Grade" Diffie-Hellman (DHE_EXPORT) mit 512-Bit-Primzahlen – ein Relikt der Krypto-Exportbeschränkungen der 90er Jahre.[20]
- **Der Mechanismus:** Ein MotS-Angreifer kann das TLS-Paket modifizieren, um dem Server vorzutäuschen, der Client wünsche Export-Verschlüsselung. Der Server sendet dann einen schwachen 512-Bit-Schlüssel.
- **Vorberechnung (Precomputation):** Das Entscheidende ist, dass eine enorme Anzahl von Servern weltweit dieselben wenigen Primzahlen für den Schlüsselaustausch nutzt (oft Standardwerte in Apache/Nginx). Ein staatlicher Akteur kann für diese spezifischen Primzahlen den diskreten Logarithmus im Voraus berechnen (was etwa eine Woche auf

einem Supercomputer dauert).[21]

- **HNDL-Implikation:** Sobald diese Vorberechnung abgeschlossen ist, kann der Angreifer den Sitzungsschlüssel einer downgradeten Verbindung in Echtzeit oder *nachträglich* (aus dem Speicher des UDC) binnen Minuten berechnen. Ein Downgrade auf 1024-Bit Diffie-Hellman, von dem vermutet wird, dass staatliche Akteure ihn brechen können, betrifft Millionen von HTTPS-, SSH- und VPN-Servern.[21]

4.3 Widerstandsfähigkeit von TLS 1.3

Das Protokoll TLS 1.3 wurde explizit entwickelt, um solche Downgrade-Attacken zu verhindern. Es signiert den gesamten Handshake kryptografisch; jede Manipulation durch einen Dritten würde die Signaturprüfung fehlschlagen lassen.[19] Dennoch zeigt die Telemetrie, dass in industriellen Umgebungen (SCADA, ICS) und im IoT-Bereich oft noch veraltete Stacks (TLS 1.2 oder älter) laufen, die anfällig bleiben.[24] Für HNDL bedeutet dies: Moderne Ziele sind schwieriger aktiv anzugreifen, aber die breite Masse der Legacy-Infrastruktur bleibt ein offenes Buch.

---

5. Vergleich von Quantencomputer-Architekturen

Die „Decrypt Later"-Komponente von HNDL hängt von der Verfügbarkeit leistungsfähiger Quantencomputer ab. Verschiedene physikalische Ansätze konkurrieren derzeit um die Skalierbarkeit, die nötig ist, um den Shor-Algorithmus auf kryptografisch relevanten Schlüssellängen (RSA-2048) auszuführen.

5.1 Supraleitende Qubits (Superconducting Qubits)

Dieser Ansatz wird primär von Branchenriesen wie IBM (Eagle, Osprey, Condor) und Google (Sycamore, Willow) verfolgt.[25]

- **Technologie:** Nutzung von Josephson-Kontakten (Transmon-Qubits), die supraleitende Schaltkreise bilden.
- **Vorteile:** Sehr schnelle Gatter-Operationen im Nanosekundenbereich. Die Fertigung ähnelt der etablierten Halbleitertechnik.
- **Herausforderungen:**
  - **Kühlung:** Die Chips müssen nahe dem absoluten Nullpunkt (Milli-Kelvin) betrieben werden. Dies erfordert riesige und teure Dilution Refrigerators.
  - **Verdrahtung:** Jedes Qubit benötigt Steuerleitungen, was bei Millionen von Qubits zu einem enormen Wärmeeintrag und Platzproblem im Kryostaten führt.
  - **Kohärenz:** Die Qubit-Zustände sind extrem flüchtig (Mikrosekunden), was eine sehr schnelle Fehlerkorrektur erfordert.[27]
- **Status:** IBM und Google haben Systeme mit >100 bis >1000 physischen Qubits

demonstriert, sind aber noch weit von der für RSA nötigen Fehlerkorrektur entfernt. Google's Willow-Chip zeigte 2024 jedoch Fortschritte in der Reduktion von Fehlerraten unter den Schwellenwert (Threshold), was Skalierung erst sinnvoll macht.[26]

5.2 Photonische Qubits (Photonic Qubits)

Unternehmen wie PsiQuantum und Xanadu setzen auf Lichtteilchen.[29] PsiQuantum verfolgt hierbei einen radikal anderen Ansatz: **Fusion-Based Quantum Computing (FBQC)**.[31]

- **Technologie:** Photonen werden durch Wellenleiter auf Siliziumchips geleitet. Statt Qubits stationär zu speichern, werden sie permanent erzeugt, durchmischen sich in Interferometern und werden gemessen.
- **Vorteile:**
  - **Raumtemperatur:** Photonen selbst benötigen keine Kühlung, um ihre Quanteneigenschaften zu behalten (nur die Detektoren benötigen Kühlung).
  - **Keine Dekohärenz im Flug:** Photonen interagieren kaum mit der Umwelt.
  - **Vernetzbarkeit:** Chips können über Glasfasern verbunden werden. Dies ermöglicht den Bau eines Quantencomputers in der Größe eines Rechenzentrums (modular), anstatt alles in einen einzelnen Kryostaten quetschen zu müssen.[33]
- **Herausforderungen:** Photonenverlust ist das Hauptproblem. Wenn ein Photon absorbiert wird, ist die Information weg. Dies erfordert massive Redundanz und komplexe Verschränkungsstrategien.
- **Status:** PsiQuantum plant aggressiv ein 1-Million-Qubit-System bis ca. 2027-2029, gestützt auf Partnerschaften mit GlobalFoundries zur Massenproduktion.[29]

5.3 Ionenfallen (Trapped Ions)

Anbieter wie IonQ und Quantinuum nutzen geladene Atome, die in elektromagnetischen Feldern schweben.[36]

- **Vorteile:** Extrem hohe Qubit-Qualität und lange Kohärenzzeiten (Sekunden bis Minuten). Jedes Ion kann mit jedem anderen verbunden werden (All-to-All Connectivity).
- **Nachteile:** Gatter-Operationen sind vergleichsweise langsam (Mikrosekunden bis Millisekunden). Die physische Bewegung von Ionen in der Falle limitiert die Skalierbarkeit auf einem einzelnen Chip massiv.

5.4 Tabelle: Hardware-Vergleich und Eignung für Kryptoanalyse

Architektur	Hauptvertreter	Gatter-Speed	Skalierbarkeit (Mio. Qubits)	Hauptrisiko für RSA-Bruch	HNDL-Zeithorizont

Supraleitend	IBM, Google	Sehr Hoch (ns)	Mittel (Kryostat-Limit)	Crosstalk, Fehlerkorrektur-Overhead	2030-2035
Photonisch	PsiQuantum, Xanadu	Lichtgeschwindigkeit	**Hoch** (Modular/Fiber)	Photonenverlust, Komponenten-Effizienz	**2027-2030** (Aggressiv)
Ionenfallen	IonQ, Quantinuum	Niedrig (µs)	Niedrig (Fallen-Größe)	Langsame Ausführung des Shor-Algorithmus	>2035

---

6. Steckbriefe: Krypto-Algorithmen und ihre Verwundbarkeit

Die HNDL-Strategie zielt auf spezifische Algorithmen ab. Hier werden die Profile der aktuellen Standards und der Downgrade-Ziele dargestellt.

6.1 Aktuelle Standards (Primärziele)

RSA (Rivest–Shamir–Adleman)

- **Typ:** Asymmetrisches Verfahren basierend auf dem Faktorisierungsproblem großer ganzer Zahlen.
- **Schlüssellängen:** 2048 Bit (Industriestandard), 4096 Bit.
- **Sicherheit:** Klassisch sicher (Faktorisierung von RSA-2048 würde klassisch Milliarden Jahre dauern).
- **Quanten-Bedrohung:** Shor-Algorithmus bietet exponentiellen Speedup.
- **Status:** RSA-2048 ist das „Hauptgericht“ für HNDL. Die weiteste Verbreitung im Web (Zertifikate) macht es zum wertvollsten Ziel.[37]

ECC (Elliptic Curve Cryptography)

- **Typ:** Asymmetrisches Verfahren basierend auf dem diskreten Logarithmusproblem elliptischer Kurven.
- **Kurven:** NIST P-256, P-384, Curve25519.

- **Sicherheit:** Effizienter als RSA (256 Bit ECC 3072 Bit RSA).
- **Quanten-Bedrohung:** Ebenfalls durch Shor angreifbar. Ironischerweise benötigen Quantencomputer für ECC oft *weniger* Qubits als für RSA vergleichbarer Stärke, was ECC im Quantenzeitalter potenziell *schwächer* macht als RSA.[38]

6.2 Downgrade-Algorithmen (Legacy & Schwachstellen)

RSA-1024

- **Status:** Von NIST und BSI als unsicher eingestuft.
- **Bedrohung:** Ein staatlicher Akteur mit massiven klassischen Ressourcen könnte RSA-1024 bereits heute oder in sehr naher Zukunft faktorisieren. Spezielle Hardware-Designs (wie das hypothetische TWIRL-Gerät) könnten die Kosten drastisch senken.
- **Verbreitung:** Immer noch häufig in IoT-Geräten, Smartcards und alten SCADA-Systemen, die keine längeren Schlüssel verarbeiten können.[39]

Diffie-Hellman 1024-Bit (Gruppen 2 & 5)

- **Problem:** Die Sicherheit von DH hängt von der verwendeten Primzahl ab. Schätzungen (Logjam-Paper) legen nahe, dass das Brechen einer einzelnen 1024-Bit-Primzahl etwa 100 Millionen bis 1 Milliarde USD kosten würde (einmaliger Aufwand für die Vorberechnung). Danach können individuelle Verbindungen in Echtzeit entschlüsselt werden.[21]
- **NSA-Bezug:** Die Snowden-Dokumente deuten darauf hin, dass die NSA genau diese Fähigkeit gegen VPNs (IPSec) einsetzt, die oft Standard-1024-Bit-Gruppen verwenden.[21]

---

7. Zeitabschätzung bis zur Entschlüsselung (Time-to-Break)

Die entscheidende Variable für HNDL ist die Zeit T, die Daten gespeichert werden müssen, bis eine Entschlüsselung möglich ist. Diese Zeitspanne hat sich durch theoretische Optimierungen des Shor-Algorithmus drastisch verkürzt.

7.1 Der Paradigmenwechsel: Gidney & Ekerå (2019/2021)

Bis ca. 2018 ging man davon aus, dass Hunderte Millionen oder Milliarden Qubits nötig wären. Die Forschung von Craig Gidney (Google) und Martin Ekerå hat die Effizienz des Shor-Algorithmus durch modulare Exponentiation und verbesserte Arithmetik revolutioniert.

- **Das Ergebnis:** Um eine 2048-Bit RSA-Zahl zu faktorisieren, werden theoretisch nur noch ca. **20 Millionen "noisy" (fehlerbehaftete) physische Qubits** benötigt.
- **Zeitrahmen:** Mit dieser Hardware könnte der Schlüssel in nur **8 Stunden** gebrochen

werden.[41]

7.2 Google's Update 2024: Die 1-Million-Qubit-Grenze

Neuere Arbeiten von Google Quantum AI (2024/2025) haben die Hürde weiter gesenkt. Durch Optimierungen in der Fehlerkorrektur und algorithmische Anpassungen (Approximate Arithmetic) deutet Google an, dass RSA-2048 möglicherweise mit **weniger als 1 Million physischen Qubits** gebrochen werden kann, wenn man eine längere Laufzeit (einige Tage statt 8 Stunden) akzeptiert.[25]

7.3 Prognostizierte Zeitlinie (Q-Day Estimates)

Die folgende Tabelle fasst die Prognosen basierend auf Hardware-Entwicklungsplänen (z.B. PsiQuantum, IBM) und der Effizienz der Algorithmen zusammen.

Kryptosystem	**Typische Anwendungsgebiete**	**Klassischer Bruch (Staatl. Akteur)**	**Quanten-Bruch (Aggressiv/Optimistisch)**	**Quanten-Bruch (Konservativ)**	**Risiko-Bewertung**
RSA-1024	Veraltete Web-Systeme, ältere Chipkarten, Legacy-VPNs (Altlasten)	Möglich (Hoher Aufwand)	~2026-2028 (Erste fehlertolerante Prototypen)	2030+	**Extrem Hoch** (Daten von heute sind akut gefährdet)
RSA-2048	Aktueller Web-Standard (HTTPS/TLS), Software-Signaturen, digitale Ausweise	Praktisch Unmöglich	~2029-2032 (Skalierung PsiQuantum/Google)	2035-2040	**Hoch** (Strategische Relevanz für HNDL*)
ECC-256	Blockchains (Bitcoin, Ethereum), Messenger (WhatsApp/Signal),	Unmöglich	~2028-2031 (Weniger Qubits	2035+	**Hoch** (Basis vieler moderner

	Mobilgeräte		nötig als RSA)		Netzwerke)
AES-256	Festplattenverschlüsselung (BitLocker/FileVault), Top-Secret Dokumente	Sicher	Unwahrscheinlich (Grover bringt nur Wurzel-Speedup)	Sicher	**Gilt als quantensicher**

**HNDL = "Harvest Now, Decrypt Later" (Jetzt sammeln, später entschlüsseln)*

Interpretation:

Daten, die heute (2025) im Utah Data Center gespeichert werden und mit RSA-2048 geschützt sind, haben eine geschätzte Halbwertszeit der Sicherheit von nur noch 5 bis 10 Jahren. Für strategische Geheimnisse (Nuklearpläne, Identitäten von Agenten), die 20+ Jahre geheim bleiben müssen, ist die aktuelle Verschlüsselung bereits heute unzureichend.

---

8. Fazit

Die Untersuchung der Infrastruktur für „Harvest Now, Decrypt Later“ offenbart ein hochgradig integriertes System aus physischer Speicherung, Netzwerküberwachung und offensiver Kryptoanalyse.

1. **Speicherinfrastruktur:** Das Utah Data Center bietet mit seiner Kombination aus massivem Energiebudget und Tape-Library-Technologie die notwendige Kapazität (Exa-/Zettabytes), um globalen Verkehr selektiv über Jahrzehnte zu archivieren.
2. **Angriffsvektoren:** Die Überwachung erfolgt primär am Internet-Backbone („Upstream“), nicht an den DNS-Root-Servern. Die Fähigkeit der NSA zu aktiven Man-on-the-Side-Angriffen (QUANTUMINSERT) begünstigt Downgrade-Attacken massiv. Durch das Erzwingen schwächerer Verschlüsselung (Logjam/Export-Ciphers) wird der Aufwand für die spätere Entschlüsselung von „Quanten-Niveau“ auf „Supercomputer-Niveau“ gesenkt.
3. **Krypto-Zukunft:** Die Entwicklung im Bereich Quantencomputing, insbesondere durch photonische Ansätze (PsiQuantum) und optimierte Algorithmen (Gidney/Ekerå), hat den erwarteten Zeitpunkt für den Bruch von RSA-2048 drastisch nach vorne korrigiert (potenziell ~2030).

Organisationen müssen daraus ableiten, dass die Vertraulichkeit von Daten, die über öffentliche Netze gesendet werden, ohne den Einsatz von Post-Quantum-Kryptografie (PQC) und Perfect Forward Secrecy (PFS) langfristig nicht mehr gewährleistet werden kann. HNDL ist keine theoretische Bedrohung der Zukunft, sondern eine operative Realität der Gegenwart.

Referenzen

1. Utah Data Center - Wikipedia, Zugriff am Januar 8, 2026, https://en.wikipedia.org/wiki/Utah_Data_Center
2. NSA Utah Data Center - Serving Our Nation's Intelligence Community, Zugriff am Januar 8, 2026, https://nsa.gov1.info/utah-data-center/
3. This mentioned the NSA's "Mission Data Repository" in Bluffdale, Utah. They ment... | Hacker News, Zugriff am Januar 8, 2026, https://news.ycombinator.com/item?id=8174937
4. Will NSA's Utah Data Center be able to handle and process five zettabytes of data?, Zugriff am Januar 8, 2026, https://skeptics.stackexchange.com/questions/16829/will-nsas-utah-data-center-be-able-to-handle-and-process-five-zettabytes-of-dat
5. There are not 13 root servers - icann, Zugriff am Januar 8, 2026, https://www.icann.org/en/blogs/details/there-are-not-13-root-servers-15-11-2007-en
6. Root name server - Wikipedia, Zugriff am Januar 8, 2026, https://en.wikipedia.org/wiki/Root_name_server
7. How Secure are the Root DNS Servers? - Brown University Department of Computer Science, Zugriff am Januar 8, 2026, https://cs.brown.edu/courses/cs180/static/files/lectures/readings/lecture7/Security%20of%20Root%20DNS%20Servers.pdf
8. DNS Log Gam At 13 Core Servers Just Unnecessary Traffic - Space Daily, Zugriff am Januar 8, 2026, https://www.spacedaily.com/reports/DNS_Log_Gam_At_13_Core_Servers_Just_Unnecessary_Traffic.html
9. Upstream vs. PRISM - Electronic Frontier Foundation, Zugriff am Januar 8, 2026, https://www.eff.org/pages/upstream-prism
10. The NSA Has Taken Over the Internet Backbone. We're Suing to Get it Back. | ACLU, Zugriff am Januar 8, 2026, https://www.aclu.org/news/national-security/nsa-has-taken-over-internet-backbone-were-suing-get-it-back
11. Glenn Greenwald: how the NSA tampers with US-made internet routers - The Guardian, Zugriff am Januar 8, 2026, https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
12. Tailored Access Operations - Wikipedia, Zugriff am Januar 8, 2026, https://en.wikipedia.org/wiki/Tailored_Access_Operations

13. Monitoring Root DNS Prefixes - ThousandEyes, Zugriff am Januar 8, 2026, https://www.thousandeyes.com/blog/monitoring-root-dns-prefixes
14. Surveillance without Borders: The "Traffic Shaping" Loophole and Why It Matters, Zugriff am Januar 8, 2026, https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/
15. Deep dive into QUANTUM INSERT – Fox-IT International blog, Zugriff am Januar 8, 2026, https://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/
16. Captures and Analysis of the QUANTUMINSERT Attack - QA Cafe, Zugriff am Januar 8, 2026, https://www.qacafe.com/resources/quantuminsert-analysis-capture/
17. Recreating the NSA's QuantumInsert attack technique - Hoxhunt, Zugriff am Januar 8, 2026, https://hoxhunt.com/blog/nsa-cyber-attack-recreating-the-quantuminsert-to-phish-gmail-on-ios
18. Why is TLS susceptible to protocol downgrade attacks? - Cryptography Stack Exchange, Zugriff am Januar 8, 2026, https://crypto.stackexchange.com/questions/10493/why-is-tls-susceptible-to-protocol-downgrade-attacks
19. Downgrade Attacks | CyberArk, Zugriff am Januar 8, 2026, https://www.cyberark.com/what-is/downgrade-attacks/
20. Logjam Attack: What You Need to Know | DigiCert.com, Zugriff am Januar 8, 2026, https://www.digicert.com/blog/logjam-attack
21. Weak Diffie-Hellman and the Logjam Attack, Zugriff am Januar 8, 2026, https://weakdh.org/
22. NSA - A Few Thoughts on Cryptographic Engineering, Zugriff am Januar 8, 2026, https://blog.cryptographyengineering.com/category/nsa/
23. TLS 1.3 - Status, Concerns & Impact - A10 Networks, Zugriff am Januar 8, 2026, https://www.a10networks.com/blog/tls-13-status-concerns-impact/
24. Legacy in Handshake: Understanding TLS 1.2 Prevalence and Its Operational Risks, Zugriff am Januar 8, 2026, https://www.sans.org/blog/legacy-handshake-understanding-tls-prevalence-operational-risks
25. Google Researcher Lowers Quantum Bar to Crack RSA Encryption, Zugriff am Januar 8, 2026, https://thequantuminsider.com/2025/05/24/google-researcher-lowers-quantum-bar-to-crack-rsa-encryption/
26. Meet Willow, our state-of-the-art quantum chip - Google Blog, Zugriff am Januar 8, 2026, https://blog.google/technology/research/google-willow-quantum-chip/
27. 9 Types of Qubits Driving Quantum Computing Forward [2025] - SpinQ, Zugriff am Januar 8, 2026, https://www.spinquanta.com/news-detail/main-types-of-qubits
28. What is the ACTUAL significance of Google's "Willow" Quantum Computing chip? - Reddit, Zugriff am Januar 8, 2026,

https://www.reddit.com/r/AskEngineers/comments/1hb8snm/what_is_the_actual_significance_of_googles_willow/
29. PsiQuantum, Zugriff am Januar 8, 2026, https://postquantum.com/quantum-computing-companies/psiquantum/
30. Xanadu Advances to Stage B of DARPA's Quantum Benchmarking Initiative, Securing up to $15 Million in Funding, Zugriff am Januar 8, 2026, https://www.xanadu.ai/press/xanadu-advances-to-stage-b-of-darpas-quantum-benchmarking-initiative-securing-up-to-15-million-in-funding
31. PsiQuantum's Path to 1 Million Qubits - HPCwire - Since 1987 – Covering the Fastest Computers in the World and the People Who Run Them, Zugriff am Januar 8, 2026, https://www.hpcwire.com/2022/04/21/psiquantums-path-to-1-million-qubits-by-the-middle-of-the-decade/
32. arXiv:2101.09310v1 [quant-ph] 22 Jan 2021, Zugriff am Januar 8, 2026, https://arxiv.org/pdf/2101.09310
33. Zugriff am Januar 8, 2026, https://postquantum.com/quantum-modalities/superconducting-qubits/#:~:text=Superconducting%20vs.,-Photonic%20Qubits&text=The%20big%20advantage%20of%20photonic,and%20potentially%20for%20optical%20computing.
34. Quantum Computing Modalities: Photonic QC, Zugriff am Januar 8, 2026, https://postquantum.com/quantum-modalities/photonic-quantum-computing/
35. PsiQuantum Is Closing In On Fault-Tolerance And A Million Qubits - Moor Insights & Strategy, Zugriff am Januar 8, 2026, https://moorinsightsstrategy.com/psiquantum-is-closing-in-on-fault-tolerance-and-a-million-qubits/
36. Quantum computing: foundations, algorithms, and emerging applications - Frontiers, Zugriff am Januar 8, 2026, https://www.frontiersin.org/journals/quantum-science-and-technology/articles/10.3389/frqst.2025.1723319/full
37. Transport Layer Security - Wikipedia, Zugriff am Januar 8, 2026, https://en.wikipedia.org/wiki/Transport_Layer_Security
38. Calculating resource estimates for cryptanalysis - Microsoft Quantum, Zugriff am Januar 8, 2026, https://quantum.microsoft.com/en-us/insights/blogs/resource-estimation/calculating-resource-estimates-for-cryptanalysis
39. State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally, Zugriff am Januar 8, 2026, https://iot-analytics.com/number-connected-iot-devices/
40. DESIGNING ENERGY-EFFICIENT CRYPTOGRAPHIC ... - IRJMETS, Zugriff am Januar 8, 2026, https://www.irjmets.com/upload_newfiles/irjmets70800032550/paper_file/irjmets70800032550.pdf
41. (PDF) How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Zugriff am Januar 8, 2026,

https://www.researchgate.net/publication/350910758_How_to_factor_2048_bit_RSA_integers_in_8_hours_using_20_million_noisy_qubits
42. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits - arXiv, Zugriff am Januar 8, 2026, https://arxiv.org/pdf/1905.09749