Bulletin of the Atomic Scientists

ISSN: 0096-3402 (Print) 1938-3282 (Online) Journal homepage: www.tandfonline.com/journals/rbul20

Quantum won't protect critical telecom networks from massive attacks. Good old maintenance might

Juljan Krause

To cite this article: Juljan Krause (2026) Quantum won't protect critical telecom networks from massive attacks. Good old maintenance might, Bulletin of the Atomic Scientists, 82:5, 361-368, DOI: 10.1080/00963402.2026.2718010

To link to this article: https://doi.org/10.1080/00963402.2026.2718010

Published online: 08 Sep 2026.

BULLETIN OF THE ATOMIC SCIENTISTS
2026, VOL. 82, NO. 5, 361–368
https://doi.org/10.1080/00963402.2026.2718010

Quantum won't protect critical telecom networks from massive attacks. Good old maintenance might

Juljan Krause

ABSTRACT

Since at least 2021, the Chinese state-sponsored campaign known as Salt Typhoon lived inside American and allied telecommunications networks, reading call records and tracking the movements of millions of people. In the aftermath, vendors, expert witnesses, and industry analysts have promoted quantum security as a new remedy, and two executive orders signed in June 2026 have given the technology fresh political momentum. An audit tested the potential impact of quantum security against the documented evidence. Of the 42 attack techniques recorded in an advisory co-signed by 23 intelligence agencies from 13 countries, quantum protections could have prevented or detected nine under the most generous reading and three under a strict one. At least 33 required administrative control of network devices, which no encryption standard, quantum or otherwise, can revoke. The attackers never broke encryption but held valid administrator credentials for long periods of time and entered through vulnerabilities that went unpatched for many years, revealing deeper structural failings. Cybersecurity budgets and attention follow novelty, while patch management and credential hygiene, whose measure of success is that nothing happens, often go unrewarded. Quantum modernization should be the graduation prize for operational discipline, never a substitute for it.

KEYWORDS

Salt Typhoon; cyber-attacks; quantum key distribution; telecommunications security; critical infrastructure protection; national security

If you own a phone, there's a fair chance that Chinese intelligence knows who you called last year (Jaikaran 2025). That's because since at least 2021 a group linked to China's Ministry of State Security (MSS) had infiltrated telecommunications networks in the United States and allied countries and spied on Americans at home and abroad. Whether anyone is still listening today, nobody in Washington can say with full confidence, and some lawmakers fear the threat is still ongoing (US Senate Committee on Commerce, Science, and Transportation 2025). The agents of the spying campaign known as Salt Typhoon spent at least four years inside America's largest telecommunications carriers, where they read call records and tracked the movements of millions of people. They even tapped the systems that carriers operate for court-ordered wiretaps (Krouse et al. 2024). Officials have concluded that the attackers "may have stolen data from almost every American" (Goldman 2025).

In the aftermath, a powerful sales narrative has taken shape: to use quantum technology and quantum hardware to prevent large-scale attacks on critical telecommunications infrastructure. The massive breach, unprecedented in scale and sophistication, was best met with new technology because new is good and probably better, the argument goes, and the most futuristic technology currently on offer is quantum.

Quantum security is a family of products that borrow from quantum physics, the science of how matter and energy behave at subatomic, atomic, and molecular scales, to protect information as it travels. Some of it is software, rewritten so that a future quantum computer cannot unpick it. Some of it is specialist hardware that sends secret keys one particle of light (photon) at a time, under the theory that any eavesdropper who intercepts a particle disturbs it and gives the game away.

Vendors urged carriers to upgrade to quantum-safe methods as a matter of survival (Rowley 2026); expert witnesses before Congress linked the breach to quantum vulnerabilities (US House Oversight and Government Reform Committee 2025), and the trade press reported that major operators began actively shopping for quantum security products (Krásová 2025). Industry analysts forecast that network operators worldwide will spend $6.3 billion on quantum hardware (chiefly quantum key distribution, the photon-by-

CONTACT Juljan Krause jkrause@gatech.edu

photon method just described) between 2025 and 2030 (Juniper Research 2025) and a whopping $23 billion by 2034 (Sharma 2026).

The narrative received a formidable boost in June, when President Trump signed two executive orders on quantum technology. One accelerates the federal migration to quantum-resistant encryption, which means replacing the mathematical locks that guard government data with new ones a quantum computer cannot pick (The White House 2026a). The other pledges to supercharge the American quantum industry (The White House 2026b). Both are welcome and address a seismic threat because one day, a good enough (or so-called "cryptographically relevant" (Palo Alto Networks 2026)) quantum computer will eventually break much of the public-key encryption in use today—the system that lets two strangers who have never met agree on encryption keys over an open line and that quietly protects almost every online activity, banking session, login, and phone call. Presidential attention casts a halo, so when The White House, for all the right reasons, elevates a technology twice in a single month, every vendor pitch gets easier and every budget line that features it becomes safer to defend and more sensible to approve. Against such momentum, challenging questions about its efficacy become harder to ask.

An audit of the Salt Typhoon campaign tested the quantum promise against the documented evidence and found that quantum security could have prevented or detected just over 21 percent of the attack techniques the hackers deployed at the most generous reading and around 7 percent at the strictest (Krause 2026). At least 33 of the 42 techniques required administrative control of network devices, which no encryption standard, quantum or otherwise, can revoke. The attackers never had to defeat encryption in the first place because they held high-level administrator credentials for years, turned the equipment's own features against its owners, and got in through vulnerabilities that had carried available patches for quite some time (seven years in an extreme case) that were never implemented, leaving carriers significantly exposed.

Quantum technology is certainly not worthless. Rather, buying it before fixing basic cybersecurity flaws due to failed patching inverts the order of operations, and the incentives pushing organizations to do exactly that are structural.

The issue is not with the policy and intelligence communities either. The engineers who wrote the joint advisory on Salt Typhoon (CISA 2025), the teams who worked on the remediation, and a great many officials across government understand the trade-offs around finite budgets and infinite purchase wish lists perfectly well and typically push back against the pull of novelty for the sake of novelty alone.

The danger lies elsewhere. The concern here is with the sales narrative around quantum, and with what such narratives do to institutions once they take hold: They bend budgets and can reset what counts as a serious cyber defense proposal. The shiny object problem is the old mistake of treating the speedy purchase of tomorrow's technology as a substitute for the maintenance of today's. Salt Typhoon is an extremely instructive empirical record of what that substitution costs.

Quantum hardware and software

What the quantum narrative sells as comprehensively quantum-securing critical networks typically bundles two very different things: The first is largely a gigantic software migration effort, the second is an expensive bet on clunky hardware.

The software migration effort implements post-quantum cryptography, novel encryption systems to protect data against codebreaking by future quantum machines while running on the computers, laptops, phones and smart devices people already own. It is therefore deployed as software, protocol and standards updates on existing compute infrastructure. The leading schemes, finalized by the National Institute of Standards and Technology (NIST) as US federal standards in August 2024 (NIST 2024), rest on lattice problems, which are geometric puzzles set in regular grids of points in hundreds of dimensions that nobody has (yet) learned to solve efficiently, quantum computer or not. That hardness is assumed rather than proven, but after decades of failed attempts at cracking lattice problems, these new standards should hold for many years to come. Nothing about post-quantum cryptography is physically quantum, however, as the new encryption schemes don't rely on the quantum-mechanical properties that give quantum technologies their power; they just happen to be complicated enough even for quantum computers.

The second of this bundling is quantum hardware, typically quantum key distribution, which exchanges keys by exploiting the physics of single photons. Two parties send each other individual particles of light down a fiber, and because the act of measuring a particle of light changes it, an eavesdropper who intercepts one leaves a mark behind. The two parties compare notes, spot the disturbance, and throw the compromised key away. In theory this offers security regardless of the attacker's computing power, even if infinite (Renner, Gisin, and Kraus 2005). The framing reliably draws audible gasps at conference talks and sales pitches, though the speakers rarely mention that at endpoints where quantum channels meet ordinary computers, these wonderful guarantees of total security meet their sudden demise. The "secured by the laws of physics" label often stretches further to quantum random number generators and attestation schemes for hardware security modules. Quantum random number generators spit out numbers that are truly unpredictable rather than merely hard to guess, which is what a good key needs. Attestation schemes make sure that the tamper-resistant boxes holding an organization's most precious keys have not been interfered with.

Throughout what follows, quantum security means that whole bundle, software and hardware together, because the bundle is what is increasingly being sold. The price tag, and the loudest pitch, usually sit at the hardware end.

Could either of these two bundles have taken the wind out of the attackers' sails and reduced Salt Typhoon to a gentle breeze? How much of Salt Typhoon exactly would quantum security have stopped? An audit published in *IEEE Security & Privacy* in June ran that quantum reality check (Krause 2026). It collected all 42 attack techniques that the Salt Typhoon hackers deployed against American and allied networks, as documented in an advisory that considers Salt Typhoon so serious that 23 intelligence agencies from 13 countries took the unprecedented step of co-signing it (CISA 2025). For each technique the hackers used, the audit asked, would stronger encryption on the wire, quantum or otherwise, have stopped this?

Under the most generous reading, quantum-securing critical telecommunications infrastructure could have prevented or detected nine of the 42 techniques. Under a strict reading anchored in what the attackers actually did, the number falls to three. Only a single technique out of 42 is plausibly preventable by quantum-channel protections alone. No matter how one counts, at least 33 techniques required administrative control of network devices, which no encryption standard can revoke, even if it is quantum powered.

The patience asymmetry

The Salt Typhoon hackers were anything but vulgar smash-and-grab thieves. They certainly did not overwhelm America's and allied cyber defenses by force or insane novelty or ingenuity. Instead, they were remarkably smooth and silent.

The state-sponsored actors lived quietly inside carrier networks and used the equipment's own administrative features rather than custom malware. They switched on the traffic-mirroring functions that routers provide for legitimate diagnostics, so that copies of live traffic could flow unnoticed to external collection points of their choosing. The Salt Typhoon actors also built tunnels similar to those that network engineers create every day, which made their massive data exfiltration look like routine intersite traffic, leaving no suspicious audit trail.

Nothing appeared out of place, because the actors "owned" administrative devices in the sense that they held valid administrator credentials at very high levels, passing as smartly dressed senior executives allowed to make and change the rules as they deem fit, no questions asked. Imagine a bank building a better, bigger, more secure vault at one of its branches. If the managers who sign off on the design hold the combination and decide who else may have it turn out to be robbers in disguise, then, the new vault is no obstacle to them at all. In the end, the shareholders have bought a thicker door and are footing the bill that came with it but gained nothing.

The hackers' remarkable patience and steadfastness deserve emphasis (and professional acknowledgment) because patience and steadfastness are what the defending side lack. Every clock on the American side runs fast. News cycles are measured in hours, budget cycles in 12 months, and political appointments in two to four years. Salt Typhoon ran for at least half-a-decade. An adversary that thinks in five-year increments will have studied a country that measures its attention in headlines and China bet, correctly, that persistence and patience would go a long way. Salt Typhoon shows that patience turns out to be an

asymmetric capability. It cost the attacker almost nothing while the defending institutions were structurally not well positioned to absorb it.

What the audit found

Every documented Salt Typhoon attack technique falls into one of two categories. Channel techniques attack traffic as it moves between devices, the way a wiretap on a trunk line would. Device techniques attack the routers, gateways, and management servers themselves. The distinction matters greatly because quantum security protects channels, brilliantly so. But it can do (almost) nothing for a device that an adversary already administers. A new, unpickable lock surely is a fine investment, unless of course the intruder has been living in the house since 2021.

The audit classified six of the 42 techniques as candidate channel attacks, the kind that would invite quantum protection. Network sniffing, for instance, evokes a passive tap on a backbone fiber, the threat quantum links are designed to expose. In practice, however, the sniffing was performed by the compromised routers themselves, which decrypted traffic as part of their normal duties and handed copies to the intruders. The wire only ever carried valid, properly encrypted flows. A quantum-secured link between two routers the adversary controls will have no choice but to protect the adversary's traffic as faithfully as anyone else's. In all six cases, the advisory's evidence shows the techniques were executed from devices under the attackers' control (CISA 2025).

Any single safeguard, audited in isolation, will look humble against a layered and sustained campaign built to defeat single controls, and that was a deliberate methodological choice. The same test applied to access management, the discipline of who may log into critical devices and do what, reveals it as the primary obstacle to 11 of the 42 techniques. The four operational classes of control together stand primary against 33. Cryptographic measures of any kind, quantum or classical, are primary against three. The point of the audit was to produce a ranking, not a summary verdict on individual controls, and regrettably, quantum sits at the bottom.

But how did the attackers gain administrative control in the first place? One finding is difficult to stomach even for seasoned cyber defenders: a vulnerability in a Cisco network feature that the company patched in March 2018 was still exploitable in August 2025 (NIST 2018). For seven years, the fix was readily available, but some of the most sensitive networks in the country would not implement it.

Salt Typhoon breached at least nine American carriers, among them Verizon, AT&T, and Lumen, with Charter, Consolidated Communications, and Windstream named in subsequent reporting (Gatlan 2025; Lyons 2025). Senators traced the failures to rudimentary gaps in patching, passwords, and authentication. Notably, AT&T and Verizon both declined a lawmaker's request for documentation showing the intruders were fully gone (US Senate Committee on Commerce, Science, and Transportation 2026), and both reportedly blocked the forensics firm that examined their networks from sharing its findings with Congress (DiMolfetta 2026). The very same telecoms industry that fell victim to Salt Typhoon at unprecedented scale, meanwhile, is accelerating its quantum efforts (Baculard et al. 2026).

The shiny object problem

In January 2025, the Federal Communications Commission ruled that carriers' statutory wiretap obligations required them to secure their networks against unlawful access and interception. They argued that carriers could hardly meet that obligation without basic measures such as multifactor authentication, strong password controls, and timely patching (US Federal Communications Commission 2025a). The Commission also proposed requiring carriers to certify annually the implementation of cybersecurity and risk-management plans (US Federal Communications Commission 2026).

These measures very much addressed the kinds of weaknesses that had sown the seeds of Salt Typhoon. But industry associations petitioned for reconsideration, and in November 2025, a newly constituted Commission rescinded the ruling and abandoned the proposed regulations, declaring them unlawful and favoring voluntary collaboration instead (US Federal Communications Commission 2025b). The Commission's current leadership argues that compliance checklists create unnecessary red tape and divert scarce resources from real defense (Johnson 2025).

Rescinding the mandate massively amplified the shiny object problem. Why sweat through tedious voluntary collaboration when regulators no longer insist on it, and an exciting technological fix glitters on the horizon? The PR is so much better, too. Quantum investments can be announced to much fanfare. They come with press conferences, Instagram stories, ribbon cuttings, and attach an organization and its senior leadership to what is one of the coolest tech words in the English language today.

The same cannot be said about the tedious job of patch management. Its measure of success is that nothing happens, and only very few people, if any, will have ever been promoted for the breach that did not occur. Presidents now sign executive orders about quantum, but no president has ever signed an executive order about finding a better password and applying software updates on time.

The pattern measurably extends far beyond telecommunications. The US federal government spends more than $100 billion a year on information technology, roughly 80 percent of it on operating and maintaining existing systems, yet government auditors keep finding critical legacy systems that run unsupported software with known security vulnerabilities (GAO 2025). Of the 10 federal legacy systems flagged in 2019 as most urgently in need of modernization, only three had been modernized by early 2025. Money follows announcements, and attention follows novelty. Scholars of infrastructure protection have documented this curious bias for years. Societies reward innovation and neglect maintenance, then everyone clutches their pearls when the bridge cracks (Vinsel and Russell 2020).

The unglamorous program to remove Chinese-made equipment from rural communication networks across America tells the same story. It pitifully limped along for years through a $3 billion funding shortfall, with rural providers reportedly forced to choose between removing suspect gear and keeping emergency services online (Dou 2024).

The misallocation involves money and scarce human attention alike. Globally, one-third of organizations report that they cannot adequately staff their cybersecurity teams, and nearly nine in 10 cybersecurity professionals say their organization has suffered at least one significant incident because of skills gaps (2025). Demands on defenders grow rapidly every year, but their budgets do not. An industry that could not apply a 2018 patch by mid-2025 is now actively shopping for quantum products (Krásová 2025). If timely patching is already overwhelming, implementing quantum hardware will be an enormous uphill struggle.

Salt Typhoon was not an outlier, either. Volt Typhoon, its better-known cousin prepositioned in American critical infrastructure, poses a strategically different problem, yet its documented tradecraft shows the same device-centric pattern (CISA 2024). So do the Russian military intelligence campaigns VPNFilter and Cyclops Blink, which compromised hundreds of thousands of routers and firewalls worldwide (Cisco Talos 2018; NCSC 2022). Two rival intelligence services with different strategic objectives independently converged on the same tradecraft, and that alone should give any cybersecurity procurement committee a moment to pause and reflect. Adversaries go where the infrastructure is weakest, and that is on poorly managed devices, not the channels between them.

A final irony is worth noting. No state has bet more heavily on quantum communication than China, which operates the world's largest quantum-encrypted network (US-China Economic and Security Review Commission 2025), some 12,000 kilometers of it, and put the first quantum satellite into orbit (Liao et al. 2017). Beijing built all of this to deny exactly the kind of interception that quantum security defeats, so nobody understands better what quantum can achieve and what it cannot. Yet when China's intelligence services reached for live access to communications and emptied nearly all of America's call records, their documented tradecraft ignored the channel layer entirely, targeting network nodes instead.

This says nothing about passive bulk collection, which China very likely also pursues, anticipating the arrival of cryptographically relevant quantum computers for future decryption, a threat worth taking seriously in its own right (Tibbetts 2020). But for the threat that actually materialized, Salt Typhoon shows where modern networks are weakest, in the considered judgment of the world's most quantum-literate adversary. It would be strange to spend billions of dollars disagreeing with them.

Fix the door first, then install that fancy new lock

Migrating to quantum-resistant algorithms is not hype but an urgent task, and the executive order that accelerates it deserves applause, but the expensive end of the quantum portfolio is a different story. Hardware that exploits quantum physics for key exchange features prominently in vendor pitches, yet the

National Security Agency and its British counterpart explicitly discourage it for government and mission-critical systems (US National Security Agency 2026).

A single specialist photon detector that protects links (and a critical telecommunications network will need plenty) can cost $20,000 apiece (NIST 2026), and that is before all the additional plumbing such systems require, which helps explain the spending forecasts above. When the same intelligence community that exposed Salt Typhoon is cautious about endorsing one of the flagship quantum security products, telecom executives might want to ask why before signing large purchase orders.

What follows is to rethink sequencing rules. Quantum modernization should be the graduation prize for operational discipline, never a substitute for it. Before a government agency or telecoms operator commits significant resources on quantum hardware for its networks, it should be able to attest that critical fixes reach internet-facing systems within days rather than years, and that no single set of stolen credentials is enough to reconfigure a backbone router.

Quantum security implemented strategically, matched to an organization's actual attack surface, will do more for long-term safety and critical infrastructure protection than a hasty universal rollout that can only disappoint. Salt Typhoon is a remarkable success story of how a great cyber power breaches great networks, waiting calmly and patiently for the defenders to get bored with the basics or become too thinly stretched to notice. The unglamorous work of closing those gaps will remain the decisive terrain of mission-critical network infrastructure defense, as a quantum fix, however awesome, can only achieve so much. No communication channels secured by the laws of quantum physics can protect a router patched seven years late.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes on contributor

Juljan Krause is an assistant professor of digital systems and international affairs at the Georgia Institute of Technology's Sam Nunn School of International Affairs, where he researches quantum computing and communications, internet technologies, cybersecurity, and network theory. He holds a doctorate in computer science from the University of Southampton in the UK and is a former senior technology and data adviser with the British government. His audit of the Salt Typhoon campaigns appeared in *IEEE Security & Privacy* in June 2026 and is available open access.

References

Baculard, Laurent-Pierre, Frank Ford, Velu Sinha, and Alex Bhak. 2026. "How Telecom Carriers Are Preparing for Quantum." Bain & Company Brief. June 5. https://www.bain.com/insights/how-telecom-carriers-are-preparing-for-quantum/.

Cisco Talos. 2018. "New VPNFilter Malware Targets at Least 500K Networking Devices Worldwide." Cisco Talos Blog. May 23. https://blogs.cisco.com/security/talos/vpnfilter.

CISA [Cybersecurity and Infrastructure Security Agency]. 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." Advisory AA24-038A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CISA [Cybersecurity and Infrastructure Security Agency]. 2025. "Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System." August 27. Joint Cybersecurity Advisory AA25-239A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a. Full advisory PDF at https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf.

DiMolfetta, D. 2026. "Senator Says AT&T and Verizon Blocked Release of Salt Typhoon Security Reports." *NextGov/FCW Magazine*, February 3. https://www.nextgov.com/cybersecurity/2026/02/senator-says-t-and-verizon-blocked-release-salt-typhoon-security-reports/411172/.

Dou, E. 2024. "Funding Shortfall for New Tech Endangers Rural Cell Service, FCC Says." *The Washington Post*, May 2. https://www.washingtonpost.com/technology/2024/05/02/huawei-rip-remove-order-threatens-service/.

Gatlan, S. 2025. "Chinese Hackers Also Breached Charter and Windstream Networks." *Bleeping Computer Magazine*, January 5. https://www.bleepingcomputer.com/news/security/charter-and-windstream-among-nine-us-telecoms-hacked-by-china/.

Goldman, A. 2025. "'Unrestrained' Chinese Cyberattackers May Have Stolen Data from Almost Every American." *The New York Times*, September 4. https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html.

ISC2. 2025. "2025 ISC2 Cybersecurity Workforce Study." December 4. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study.

Jaikaran, C. 2025. "Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications." *CRS In Focus* IF12798. Washington, DC: Congressional Research Service. January 23. https://www.congress.gov/crs-product/IF12798.

Johnson, Derek B. 2025. "The Congressional Remedy for Salt Typhoon? More Information Sharing with Industry." *Cyberscoop Magazine*, December 2. https://cyberscoop.com/salt-typhoon-senate-commerce-hearing-fcc-telecom-cybersecurity/.

Juniper Research. 2025. "Quantum Key Distribution: Network Operators to Spend $6.3 Billion Over Next Six Years." January 28. https://www.juniperresearch.com/press/quantum-key-distribution-network-operators-to-spend-6bn/.

Krásová, T. 2025. "2025 in Review: Telecom Gets Entangled with Quantum." *Light Reading*, December 16. https://www.lightreading.com/security/2025-in-review-telecom-gets-entangled-with-quantum.

Krause, J. 2026. "Salt Typhoon and the Limits of 'Quantum Security': A Technique-Level Audit." *IEEE Security & Privacy* 24 (4): 59–70. https://doi.org/10.1109/MSEC.2026.3688536.

Krouse, S., D. Volz, A. Viswanatha, and Robert McMillan. 2024. "U.S. Wiretap Systems Targeted in China-Linked Hack." *Wall Street Journal*, October 5. https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

Liao, S. K., W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, et al. 2017. "Satellite-To-Ground Quantum Key Distribution." *Nature* 549 (7670): 43–47. https://doi.org/10.1038/nature23655.

Lyons, J. 2025. "Charter, Consolidated, Windstream Reportedly Join China's Salt Typhoon Victim List." *The Register*, January 6. https://www.theregister.com/security/2025/01/06/three-more-telcos-reportedly-join-china-salt-typhoon-victims/1170678.

NIST [National Institute of Standards and Technology]. 2018. "CVE-2018-0171 Detail." National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2018-0171.

NIST [National Institute of Standards and Technology]. 2024. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." August 13. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

NIST [National Institute of Standards and Technology]. 2026. "Cost Effective QKD System Developed by NIST." https://www.nist.gov/itl/cost-effective-qkd-system-developed-nist.

Palo Alto Networks. 2026. "Brief: Cryptographically Relevant Quantum Computers." https://www.paloaltonetworks.com/cyberpedia/crqcs-cryptographically-relevant-quantum-computers.

Renner, Renato, Nicolas Gisin, and Barbara Kraus. 2005. "Information-Theoretic Security Proof for Quantum-Key-Distribution Protocols." *Physical Review A* 72 (1): 012332. https://doi.org/10.1103/PhysRevA.72.012332.

Rowley, S. 2026. "KETS Quantum Security Reacts to Salt Typhoon Cyber Attacks." Blog post. https://dcnnmagazine.com/news/kets-quantum-security-reacts-to-salt-typhoon-cyber-attacks/.

Sharma, R. 2026. *Quantum Key Distribution for Telecom Market Research Report 2034*. Market Intelo Report. https://marketintelo.com/report/quantum-key-distribution-for-telecom-market.

Tibbetts, J. 2020. "Keeping Classified Information Secret in a World of Quantum Computing." *Bulletin of the Atomic Scientists*, February 11. https://thebulletin.org/2020/02/keeping-classified-information-secret-in-a-world-of-quantum-computing/.

NCSC [UK National Cyber Security Centre]. 2022. "New Sandworm Malware Cyclops Blink Replaces VPNFilter." Advisory. February 22. https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter.

US Federal Communications Commission. 2025a. "FCC to Require Carriers to Secure Networks." January 16. Press release. https://www.fcc.gov/document/fcc-require-carriers-secure-networks.

US Federal Communications Commission. 2025b. "Protecting the Nation's Communications Systems from Cybersecurity Threats." The Federal Register. Notice. December 15. https://www.federalregister.gov/documents/2025/12/15/2025-22830/protecting-the-nations-communications-systems-from-cybersecurity-threats.

US Federal Communications Commission. 2026. "Proposed FCC Rulemakings." Proceedings & Actions. https://www.fcc.gov/proposed-rulemakings.

GAO [US Government Accountability Office]. 2025. "Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems." July 17. Press release. https://www.gao.gov/products/gao-25-107795.

US House Oversight and Government Reform Committee. 2025. "Salt Typhoon: Securing America's Telecommunications from State-Sponsored Cyber Attacks." Transcript. April 2. https://www.congress.gov/event/119th-congress/house-event/118084.

US National Security Agency. 2026. "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)." Press release. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

US Senate Committee on Commerce, Science, and Transportation. 2025. "Experts Agree: U.S. Communications Networks Remain Vulnerable Following Salt Typhoon Hack." December 2. Press release. https://www.commerce.senate.gov/press/dem/release/experts-agree-u-s-communications-networks-remain-vulnerable-following-salt-typhoon-hack/.

US Senate Committee on Commerce, Science, and Transportation. 2026. "Cantwell Demands AT&T, Verizon CEOs Come Clean on Salt Typhoon Hacks, Ongoing Network Security Risks." February 3. Press release. https://www.commerce.senate.gov/press/dem/release/cantwell-demands-att-verizon-ceos-come-clean-on-salt-typhoon-hacks-ongoing-network-security-risks/.

US-China Economic and Security Review Commission. 2025. *Vying for Quantum Supremacy: U.S.-China Competition in Quantum Technologies*. Report. November 18. https://www.uscc.gov/research/vying-quantum-supremacy-us-china-competition-quantum-technologies.

Vinsel, Lee, and Andrew L. Russell. 2020. *The Innovation Delusion: How Our Obsession with the New Has Disrupted the Work That Matters Most*. New York: Crown Currency.

The White House. 2026a. "Securing the Nation Against Advanced Cryptographic Attacks." June 22. Executive Order 14412. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/.

The White House. 2026b. "Ushering in the Next Frontier of Quantum Innovation." June 22. Executive Order 14413. https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/.