Salt Typhoon and the Limits of "Quantum Security": A Technique-Level Audit

Juljan Krause | Georgia Institute of Technology

Salt Typhoon prompted urgent calls for quantum-secured telecommunications, but would it have helped? We analyze all documented attack techniques and find that 79%–93% exploited device-level vulnerabilities that "quantum security" cannot address.

In August 2025, a coalition of intelligence and cybersecurity agencies from thirteen countries issued a joint advisory detailing sustained campaigns by China-linked advanced persistent threat (APT) actors, commonly tracked as Salt Typhoon.[1] The advisory describes systematic compromises of telecommunications backbones and edge routers across multiple regions, affecting government networks, critical infrastructure, and commercial systems globally. In an unprecedented move, the 23 cosealing agencies name specific Chinese private-sector companies alleged to have carried out the campaigns on behalf of People's Republic of China (PRC) government and military actors.

The attackers obtained metadata from millions of phone users, tapped law enforcement systems, and siphoned customer call records. Active since at least 2021, the campaigns combined modification of router configurations, deployment of containers on network devices, activation of switched port analyzer (SPAN)/encapsulated remote SPAN (ERSPAN) traffic mirroring, and establishment of covert tunnels for lateral movement and data exfiltration. The campaigns also exposed private communications of high-value individuals, often political figures, campaign staff, and public officials for prolonged periods, prompting U.S. policymakers to conclude that Salt Typhoon actors "may have stolen data from almost every American."[4]

In the wake of Salt Typhoon, policy discourse and vendor narratives have identified quantum-secured networking as a primary defensive response. "Quantum security" is vendor shorthand for a spectrum of technologies: at minimum, postquantum cryptography, meaning algorithms resistant to cryptanalysis by future quantum computers, now standardized by the National Institute of Standards and Technology (NIST). More costly deployments add quantum key distribution (QKD), exploiting quantum-mechanical properties to detect interception during key exchange. At the upper end sit hardware-embedded quantum random number generators and tamper-evident key management infrastructures. Throughout this article, "quantum security" (QS) refers to this full technology stack; having defined the term, we drop the quotation marks hereafter.

Independently of Salt Typhoon, NIST and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have issued guidance on postquantum migration timelines[5,7] in response to the long-term cryptanalytic threat from quantum computing. In the aftermath of Salt Typhoon specifically, vendors have found renewed quantum urgency in the campaign, recommending enterprises and governments to "upgrade to quantum-safe methods, including a defense in depth approach with [QKD] and post quantum algorithms"[8] while expert testimony before Congress linked Salt Typhoon to quantum cryptographic vulnerabilities.[3] The outgoing U.S. Federal Communications

Digital Object Identifier 10.1109/MSEC.2026.3688536

Copublished by the IEEE Computer and Reliability Societies

Commission chair framed Salt Typhoon as a "clarion call" for network security.[6] With major telecommunications operators now actively seeking to deploy QS products on their networks,[2] these narratives are already translating into investment decisions.

The premise underlying calls to pivot to comprehensive QS is that stronger channel cryptography would have degraded Salt Typhoon's operations. Yet the U.S. National Security Agency and the U.K.'s Government Communications Headquarters explicitly discourage QKD for government and mission-critical systems, citing operational limitations and implementation risks.[9] This tension between vendor narratives and intelligence-community guidance raises a basic empirical question: how much of Salt Typhoon's documented behavior actually falls within the threat model that QS is designed to address? Put differently, *would quantum security have actually prevented Salt Typhoon's documented attack techniques?*

This article answers that question through systematic analysis of all 42 techniques documented in the joint advisory. We classify each technique as *channel-level* (requiring observation or manipulation of traffic in transit, and thus amenable to cryptographic hardening) or *device-level* (requiring administrative control of network infrastructure, where channel cryptography is largely orthogonal). The results are stark: 79%–93% of Salt Typhoon's attack surface lies on compromised infrastructure devices, leaving QS directly relevant to only 7%–21% of documented techniques. The gap exists because Salt Typhoon operated *from* compromised routers and gateways, not *against* the communication channels between them. When adversaries control the devices that terminate encrypted sessions, channel-layer protections (quantum or otherwise) provide only very limited benefit. This is because control-plane compromise fundamentally undermines cryptographic protections. When APT actors control routing and policy enforcement, defender cryptography choices become secondary.

Crucially, the Salt Typhoon campaigns achieved their objectives without relying on zero-day exploits. Initial access and persistence were gained through well-documented vulnerabilities in widely deployed systems; flaws for which patches had been available for months or years. One particularly striking example is CVE-2018-0171, a critical Cisco vulnerability patched in March 2018, which remained exploitable in August 2025, a seven-year exploitation window. The success of Salt Typhoon thus reflects not breakthrough offensive capabilities but patient exploitation of the operational gap between available defenses and their implementation. Our analysis indicates that operational controls, i.e., **access management, configuration governance, platform integrity, and network segmentation**, address roughly 11 times as many of Salt Typhoon's documented techniques by count than cryptographic hardening. A governance-first strategy would have denied far more attack techniques than a cryptography-first strategy alone.

To our knowledge, this is the first technique-level empirical audit of a state-sponsored infrastructure APT campaign evaluated through a quantum-defensive technology lens. Our goal is not at all to dismiss QS: it has clear value for protecting high-value links against passive interception and harvest-now-decrypt-later (HNDL) threats, for providing forward secrecy that protects past communications even after device compromise, and for raising adversary costs through tamper-evident signaling that increases detection risk. Rather, we aim to clarify quantum's appropriate role relative to operational controls when defending against infrastructure-targeting APTs. The question is not whether QS has value, as it clearly does, but whether it should lead or follow investment in the operational controls that address the dominant threat model.

The remainder of this article details our classification methodology, presents findings organized around three operational patterns that defined Salt Typhoon, and derives an evidence-based priority framework for telecommunications defenders. We generalize our findings for APT campaigns beyond Salt Typhoon and conclude with implications for operators, vendors, and policymakers seeking to allocate finite security budgets against documented real-world adversary behavior.

Salt Typhoon's Campaign Profile

The Salt Typhoon campaigns demonstrate patient, methodical targeting of telecommunications infrastructure over at least four years (2021–2025). The unprecedented joint disclosure by 23 intelligence agencies from 13 countries reflects both the adversary's sophisticated trade-craft and the opportunity space created by operational security gaps. The joint advisory identifies compromises across telecommunications, government, transportation, and lodging sectors, providing Chinese intelligence services with "the capability to identify and track their targets' communications and movements around the world."[1]

The scope reflects the attack surface: compromise of telecommunications backbone infrastructure provides adversaries with visibility into virtually all communications traversing affected networks. The campaigns obtained metadata from millions of phone users (call detail records, location data), access to law enforcement wiretap systems (Communications Assistance for Law Enforcement Act interfaces), private communications of high-value targets (political figures, campaign staff) as well as customer call records and billing information.

In this pursuit, the Salt Typhoon campaigns shared some common characteristics:

- *"living off the land":* abuse of legitimate features [SPAN mirroring, generic routing encapsulation (GRE) tunnels, diagnostic containers] rather than custom malware
- *control-plane focus:* manipulation of routing, access control lists (ACLs), and authentication rather than data-plane packet inspection
- *trusted interconnect exploitation:* lateral movement via high-trust provider-to-provider and provider-to-customer links
- *Persistence over disruption:* maintaining long-term access for intelligence collection rather than destructive attacks.

This operational reality, i.e., adversaries operating *from* devices rather than *against* channels, is precisely what QS is not designed to address, and motivates our classification framework: *channel* tactics (link-dependent, amenable to cryptographic hardening) versus *device* tactics (on-device control-plane manipulation, orthogonal to channel protections).

Exploitation Without Zero-Days

Remarkably, Salt Typhoon actors progressed with *no reliance on previously unknown vulnerabilities*. Instead, the campaign leveraged well-documented flaws in widely deployed systems. The most relevant common vulnerabilities and exposures (CVEs) exploited by Salt Typhoon, including patch dates, are listed in the supplementary data set available at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author.

The persistence of CVE-2018-0171 exploitation deserves particular emphasis: organizations remained vulnerable to a **seven-year-old** flaw with available remediation. Some organizations were still exposed as of August 2025.

Attack Techniques: Control-Plane Compromise

The Salt Typhoon attackers deployed specific techniques enabling persistent access and data collection, largely by compromising the *control plane* where routing, authentication, and policy decisions occur, rather than the data plane where packets are forwarded. Once the control plane is compromised, APT actors manage routing and policy enforcement, making defensive cryptography choices secondary if not irrelevant.

Attackers modified ACLs, altered routing tables, and weakened authentication settings. Because changes occurred on authoritative devices, they appeared legitimate in logs and audit trails. Standard configuration workflows failed to detect malicious changes absent cryptographic signing and dual-approval controls. APT actors also deployed containerized implants (e.g., Cisco Guest Shell) providing persistent execution environments while evading monitoring. Injected at critical aggregation points, these router-based implants provided complete visibility into traffic flows.

Salt Typhoon attackers used SPAN to mirror traffic to local interfaces and ERSPAN to send copies to remote collection points via GRE tunnels, enabling comprehensive traffic capture from compromised routers. When initiated from captured devices via authenticated comand line interfaces (CLIs), such mirroring bypasses endpoint protections entirely. GRE and Internet Protocol Security (IPsec) tunnels originating from compromised routers provided encrypted channels for lateral movement and exfiltration. These tunnels blend with legitimate network operations (VPN termination, intersite connectivity), making their discovery difficult without behavioral analytics and anomaly detection.

Classifying Attack Surfaces

We systematically analyzed all 42 documented Salt Typhoon techniques.[1] For each ATT&CK technique, we recorded the technique identifier and name, the advisory's description of how Salt Typhoon implemented it, the kill-chain phase (tactic), and the technical dependencies required for success (for example, credentials, local device access, or a specific network path).

The purpose of this exercise was to ask one concrete question: *does a stronger channel (quantum or classical) materially change the adversary's options, or is the critical control on the devices that originate, terminate, or route the traffic?* This framing provides us with a straightforward and powerful split between channel and device techniques.

The Channel Versus Device Question

Channel techniques operate on traffic flowing *between* network endpoints. An archetypal example is an HNDL attack, where an adversary passively records encrypted traffic today in the hope of decrypting it in the future with a cryptanalytic breakthrough. Quantum-resistant key establishment or QKD directly degrades the adversary's ability to succeed.

Device techniques operate *on* compromised infrastructure: routers, firewalls, VPN concentrators, management servers, or customer-facing applications. Once an adversary controls those devices, they can terminate encrypted sessions, alter routing and access-control policies, or mirror traffic in plaintext before it ever reaches a protected channel. No amount of extra QS on the wire can distinguish "legitimate" Transport Layer Security (TLS) from TLS initiated by a router the adversary already owns.

Salt Typhoon's documented operations are overwhelmingly of the second kind. Even techniques whose names suggest passive interception, e.g., *network sniffing*, were implemented via SPAN/ERSPAN sessions configured from compromised routers, not via out-of-band optical taps. In other words, most of the attack surface of this campaign targeting critical network infrastructure lives on devices, not in the channel.

How We Coded the 42 Techniques

In practical terms, we classified each technique using three rules: 1) If the technique's essential precondition is reading or modifying traffic *in transit* without compromising the endpoints (for example, a wiretap on a provider trunk), we label it channel. 2) If the technique requires creating, altering, or abusing state on routers, switches, servers, or management systems (for example, changing ACLs, pushing config, abusing guest shells, or pivoting via compromised routers), we label it device. 3) For techniques that can be implemented either way in principle, we coded them twice; once under a generous "implementation-agnostic" reading (assuming quantum-safe channels help in principle where QS theoretically addresses this attack vector class) and once under a more conservative "implementation-based" reading (anchored in Salt Typhoon's actual device-level implementations).

Only six techniques fell into this disputed category: T1040 (network sniffing), T1071 (application layer protocol), T1090 (proxy), T1090.003 (multi-hop proxy), T1095 (non-application layer protocol), and T1048.003 (exfiltration over alternative protocol). An implementation-agnostic coder might treat these as channel-level preventable because their names evoke interception or tunneling. In Salt Typhoon's case, however, the advisory evidence shows that all six were driven from compromised infrastructure under the actors' control. The following Section and Table 1 walk through the details of how these "channel-sounding" techniques actually played out on devices.

Under the implementation-agnostic coding, nine out of 42 techniques (21.4%) are judged amenable to quantum-protected channels: seven as preventable, two as detectable via attestation or hardened hardware

Table 1. Device-level implementations of channel-sounding techniques.

Technique	Sounds Like...	Actually Is...	Why This Is Device, Not Channel
T1040: Network sniffing	Passive backbone tap	SPAN/ERSPAN sessions configured from router CLI	Traffic is mirrored in plaintext by a compromised endpoint; the network only ever sees legitimate frames leaving an owned device.
T1071: Application layer protocol	On-path HTTPS interception	HTTPS C2 sessions initiated from the router	C2 uses valid TLS and application protocols originating from authenticated infrastructure the adversary controls; the channel cannot distinguish it from normal admin traffic.
T1090: Proxy	Generic "use of a proxy service"	Routers and Virtual Private Servers used as forwarding points for operator access	Proxy endpoints run on compromised hosts; once those devices are owned, the channel simply carries their traffic as designed.
T1090.003: Multi-hop proxy	Obscure multi-hop tunnel on the wire	Chained relays across multiple compromised routers and servers	Each hop is an explicit configuration change on devices; quantum-safe channels between them do not stop those devices from forwarding traffic.
T1095: Non-Application layer protocol	Low-level protocol abuse in transit	GRE/Internet Control Message Protocol-style tunnels configured on routers	Tunnel endpoints are created in router configuration; the "tunnel" is an intentional feature of owned infrastructure, not an attack on the link itself.
T1048.003: Exfiltration over alternative protocol	Sneaky alternative protocol on the backbone	Data exfiltrated over standard protocols (for example HTTPS) from managed infrastructure	Exfiltration rides on ordinary, correctly encrypted sessions launched from compromised devices; from the channel's point of view, this is just another legitimate flow.

security modules. Under the implementation-based coding, only three techniques (7.1%) remain in that category. In both cases, the remaining 33–39 techniques (78.6%–92.9%) are purely device-level; strengthening channels does not remove, or even meaningfully weaken, the corresponding attack paths.

Completeness and Rationale for Linear Counting

Our analysis covers all 42 ATT&CK techniques documented in the joint advisory.[1] This count is independently corroborated by the accompanying STIX 2.1 machine-readable data bundle published by CISA, which contains the same 42 technique-level attack-pattern objects. The advisory describes its tactics, techniques, and procedures (TTPs) compilation as covering techniques "used since at least 2021 to target enterprise environments," and represents the output of multiagency forensic investigations across 13 countries, making it the most authoritative and complete public record of the campaign available.

To rule out alternative explanations of the overwhelming dominance of device-level techniques, we note that ATT&CK as a classification framework is not inherently biased toward devices. It includes network-layer techniques, such as network sniffing (T1040) and adversary-in-the-middle (T1557) in its network devices matrix.[12] Indeed, six of our 42 techniques have outright "channel-sounding" names (Table 1); we examined each carefully in our assessment that Salt Typhoon implemented all six from compromised devices. The device-dominant distribution reflects the adversary's operational choices, not a classification artifact or an inherently device-centric framework.

Our technique counts measure how many distinct ATT&CK techniques each class of controls can address; they do not claim to capture incident frequency, loss severity, or strategic impact. A rarely used but catastrophic technique and a common reconnaissance step each contribute one to the tally. This is a deliberate methodological choice for four reasons.

1. Defenders working from public advisories will rarely enjoy having complete technique-level impact and risk weightings ready at hand; our framework demonstrates what rigorous analysis is possible from data practitioners actually possess.
2. Importantly, Salt Typhoon's dependency chains mean that high-impact channel techniques were downstream of prior device compromise ("Attacks on Critical Infrastructure: The Device-Level Reality" section, Pattern B): e.g., exfiltration over alternative protocols (T1048.003) required tunnel creation (T1572), which required device compromise (T1190). Even under impact-weighted analysis, investment sequencing does not change; the device-level prerequisites must still be addressed first.
3. A risk-weighted alternative would require per-technique loss-severity estimates and organization-specific asset valuations that are either unavailable or unreleased, requiring sector- and firm-level estimates that go beyond the pragmatic, evidence-based guidance this short article aims to provide.
4. Impact weighting risks creating dangerous blind spots: if technique x is weighted as low-impact based on one campaign's profile, defenders may deprioritize it. Yet that same technique may prove decisive in a future campaign against different infrastructure or with different objectives. All 42 techniques were actually deployed in a real-world campaign of strategic consequence; equal weighting treats each as a documented capability the adversary has demonstrated and may employ again, which is the prudent assumption when generalizing beyond a single case.

This article analyzes Salt Typhoon specifically. The degree to which the device-dominant pattern generalizes to other infrastructure-targeting campaigns is examined in detail in the penultimate section.

Attacks on Critical Infrastructure: The Device-Level Reality

Our findings challenge quantum-first defensive narratives regardless of analytical perspective. Under implementation-agnostic coding (crediting quantum for all techniques with theoretical channel-layer relevance), **79% of Salt Typhoon techniques remain device-level**, requiring administrative control unmitigated by channel cryptography. Under implementation-based coding (evaluating Salt Typhoon's documented operational implementation), **93% are device-level**, with quantum addressing only 7.1% with certainty.

Salt Typhoon adversaries operated *from* compromised routers, not *against* channels between routers, using legitimate administrative interfaces with valid credentials. Quantum channel security cannot distinguish malicious configuration changes from authorized operations when both originate from authenticated devices. A table and full classification breakdown are provided in the supplementary data set available at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author; the key distribution is captured in Figure 1.

Three Patterns That Define Salt Typhoon

Rather than catalog all 42 techniques sequentially, we discuss three patterns that reveal Salt Typhoon's

operational logic and QS's limited applicability. Full per-technique mappings are available in our companion data set available in the supplementary materials at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author.

Pattern A: Even "channel" techniques were device-executed. Read against the ATT&CK technique names alone, Salt Typhoon seems a great test case for QS. Network sniffing, application layer protocol, proxy, multi-hop proxy, non-application layer protocol, and exfiltration over alternative protocol all sound like classic "on-the-wire" problems that stronger channels ought to fix.

The advisory tells a different story. In every one of these six cases, Salt Typhoon implemented the technique from already-compromised infrastructure: routers, VPN gateways, or management systems under the actors' control. Traffic was created, mirrored, or tunneled *on* those devices, then handed to the network as perfectly valid, well-formed flows so that from the channel's perspective, nothing looked suspicious.

Table 1 shows how these "channel-sounding" techniques actually played out on devices.

These six techniques are precisely the ones that a generous, "implementation-agnostic" reading might treat as channel-preventable. Salt Typhoon shows why that optimism is misplaced. As soon as adversaries own the routers and gateways, they can sniff, tunnel, and exfiltrate entirely within the rules of whatever channel protections have been deployed. Quantum or classical, the wire just carries whatever the compromised devices decide to send.

Pattern B: Where quantum actually helps. While Pattern A shows where quantum *does not* help, Pattern B is about the narrow slice where it might. Only 1–9 out of 42 techniques (2.4%–21.4%) fall on the Channel side of the ledger, depending on the implementation perspective. The lower bound (1) counts only techniques we treat as clearly channel-preventable under a conservative, implementation-aware reading. The upper bound (9) adds cases where channel-layer controls might help with detection in best-case scenarios, but do not remove the need for device governance.

T1571 (non-standard port) is the only technique we can plausibly treat as channel/preventable in isolation. Using nonstandard ports [for example, secure shell (SSH) on 8443 instead of 22] to evade detection is a property of the traffic in transit; in principle, channel-facing controls, strict egress filtering, and tight service allowlists can flag unexpected protocols on unusual ports. In practice, once

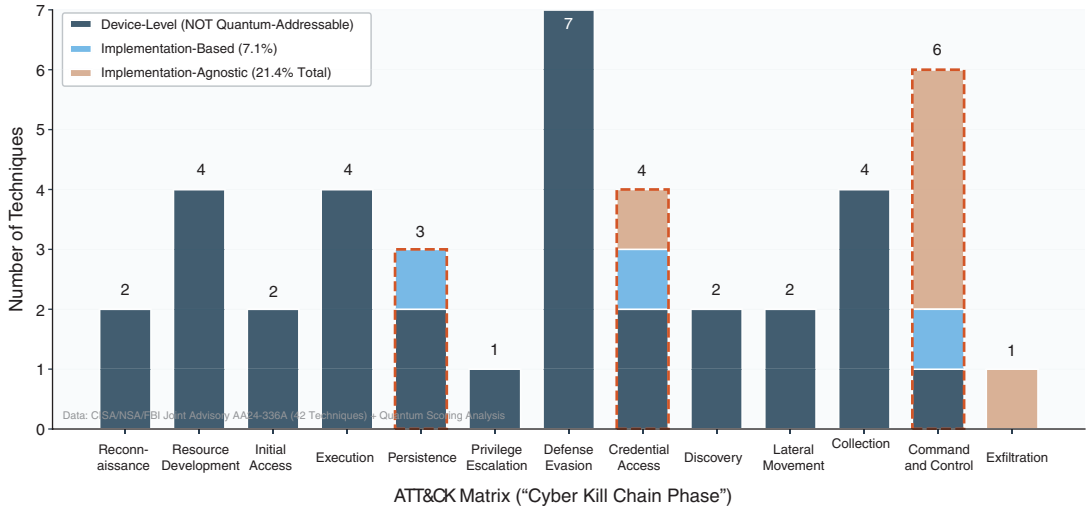

Figure 1. Salt Typhoon attack distribution across cyber kill chain phases. Device-level techniques (dark blue) requiring administrative access to compromised network infrastructure dominate all attack phases. QS addresses 3–9 techniques out of 42 (7.1%–21.4%) depending on threat model assumptions. Implementation-based bound (7.1%, light blue) includes three techniques where quantum prevents passive interception or detects cryptographic manipulation [secure shell (SSH) key insertion in "Persistence," TACACS+ server redirection in "Credential Access," and nonstandard port interception in "Command and Control"]. Implementation-agnostic bound (21.4%, tan overlay) adds six techniques in principle amenable to QS but in the actual Salt Typhoon campaigns originated from compromised devices (network sniffing, C2 proxy establishment, and alternative protocol exfiltration). Traffic originating from owned routers appears legitimate to QKD systems, collapsing the implementation-agnostic band. The 79%–93% device-level majority operates above the channel layer where QS provides no meaningful defensive value. Dashed boxes highlight phases containing quantum-addressable techniques. (Source: CISA/NSA/FBI Joint Advisory AA25-239A; used with permission).

adversaries control network devices, they can configure those nonstandard ports as authorized services, making them indistinguishable from legitimate traffic. In Salt Typhoon's operational context, segmentation and monitoring, not cryptography, are therefore the primary defenses against T1571.

T1602.001/002 [Simple Network Management Protocol (SNMP)/Management Information Base (MIB) Dump, Config Dump] sit on the management plane and *could* occur without full device compromise, e.g., when an adversary has SNMP credentials or Trivial File Transfer Protocol access but no operating system (OS)-level control. Quantum-secure channels prevent passive interception of configuration data in cases where attackers can only eavesdrop but cannot authenticate as a management client. In infrastructure APT campaigns, however, these techniques typically occur *after* initial device compromise, so classifying them as channel-relevant relies on a very narrow threat model.

T1048.003 (exfiltration over alternative protocol) uses GRE/IPsec tunnels for data exfiltration. In Salt Typhoon, those tunnels are created via T1572 (protocol tunneling), which is firmly device-level. The dependency chain is compromise device (T1190) → create tunnel (T1572, device) → exfiltrate via tunnel (T1048.003). Because the tunnel endpoints themselves require device compromise, treating T1048.003 as a channel technique reflects only the final exfiltration step, not the essential dependency.

T1040 (network sniffing) further illustrates the label-versus-implementation tension. As discussed in Pattern A, the advisory describes "passively collect[ing] packet capture," which could suggest channel-level optical taps. Salt Typhoon implemented this via SPAN/ERSPAN on compromised routers that terminated VPN tunnels, capturing post-decryption plaintext. The decisive precondition is administrative control of those devices, not the strength of channel cryptography.

This distinction matters because QS marketing assumes adversaries sit on transit links conducting passive bulk collection. This is the HNDL threat model. Salt Typhoon shows that infrastructure-centric APTs instead compromise devices at strategic network positions, i.e., tunnel endpoints, provider interconnects, or edge gateways where traffic is plaintext before encryption or after decryption. Quantum protection on backbone links between those already-compromised endpoints provides only marginal defensive value.

Salt Typhoon's initial access vectors were predominantly CVE exploitation and credential theft from device configurations rather than interception of credentials from communication channels. While the possibility that some credentials were harvested in transit cannot be excluded, the documented evidence indicates that channel hardening would not have disrupted the primary upstream device-compromise steps that enabled the campaign.

Pattern C: The seven-year exploitation window. T1190 (exploit public-facing application) enabled initial access through known CVEs: CVE-2024-21887 (Ivanti), CVE-2024-3400 (Palo Alto), CVE-2023-20198/20273 (Cisco IOS XE), and CVE-2018-0171 (Cisco Smart Install). The last is particularly striking given its seven-year exploitation window. T1068 (Privilege Escalation), T1199 (Trusted Relationship) and T1609 (Container Administration) are all device-level techniques. They too reflect **operational gaps**, i.e., the time lag between patch availability and deployment, insufficient configuration governance, and weak interconnect authentication. Patient APT actors exploit these process failures and insufficient governance structures, not cryptographic weaknesses. Ironically, organizations that would have deployed quantum-secured channels while leaving CVE-2018-0171 unpatched were to remain compromised regardless of their cryptographic sophistication. While quantum addresses *off-path eavesdroppers* conducting passive collection, Salt Typhoon represents *on-device adversaries* exploiting software vulnerabilities and weak operational discipline.

Defensive Investment Priorities: What Actually Works

For each of the 42 techniques, we identify the defensive technology classes most directly positioned to prevent or materially degrade that technique. These categories align with established security frameworks (NIST SP 800-53,[13] CIS controls[14]). To keep the taxonomy practitioner-oriented, we group controls into seven broad classes:

1. *cryptographic controls*: protocol choices, key management, and secure storage of secrets
2. *access control*: authentication, authorization, and role-based access to devices and management interfaces
3. *configuration management*: baselines, change-control processes, and configuration audit
4. *network segmentation*: logical and physical separation including routing policies, egress rules, and tunnel restrictions
5. *platform integrity*: secure boot, runtime attestation, and detection of unauthorized code or firmware
6. *patch management*: testing and deploying vendor

security fixes within acceptable timeframes.
7. *threat intelligence*: operationalization of indicators of compromise (IOCs) and adversary tradecraft to tune the other six classes.

Many techniques can in principle be mitigated by several classes of control. Rather than enumerate all possibilities, we assign a *primary* and *secondary* defensive class to each technique. The primary class reflects the control that must fail for the technique to succeed in the documented Salt Typhoon trade-craft; the secondary class is the next-most-relevant structural control. A comprehensive mapping table, alongside a rationale and explanation for each mapping decision is available in the supplementary material at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author.[a]

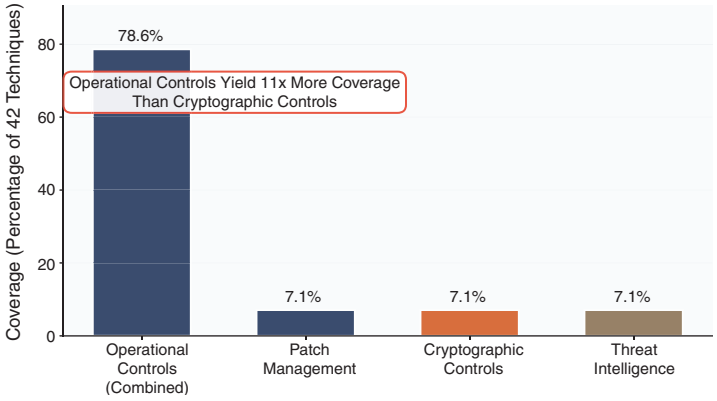

Figure 2. Defensive technology effectiveness against Salt Typhoon. Pooled operational controls (access control, configuration governance, platform integrity, network segmentation) outperform cryptographic novelty for infrastructure-centric APT campaigns 11 times by technique-count. Complete defensive technology mappings for all 42 techniques, including primary/secondary defenses, rationales, and implementation details, are available in the supplementary materials available at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author.

The Defensive Technology Landscape

Figure 2 shows which defensive technology classes address how many Salt Typhoon techniques. The findings challenge prominent narratives urging rapid quantum adoption and suggest a clear evidence-based priority hierarchy for telecommunications operators.

The empirical distribution is striking. Operational controls (access control, configuration governance, platform integrity, network segmentation pooled together) address 11-fold more distinct ATT&CK techniques than cryptographic protections alone in terms of coverage breadth. While this figure is no reflection of attack propagation, it does reflect Salt Typhoon's documented operational pattern: adversaries operated *from* compromised devices using legitimate administrative features, not *against* channels between devices through passive interception.

The Evidence-Based Priority Hierarchy

Based on our classification of all 42 techniques, we propose the following defensive investment priority, ranked by technique-count coverage (detailed mappings, rationales, and implementation guidance are available in the supplementary data set available at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author):

- *priority 1: access control (26.2%, 11 techniques)*: role-based access, least-privilege policies, SPAN/ERSPAN restrictions, and administrative action monitoring
- *priority 2: configuration management (19.0%, 8 techniques)*: signed configurations, dual-approval workflows, and immutable audit trails
- *priority 3: platform integrity (16.7%, seven techniques)*: secure boot, firmware attestation, and container restrictions
- *priority 4: network segmentation (16.7%, 7 techniques)*: zero-trust interconnects, egress filtering, and tunnel monitoring.

These four operational control classes collectively address 78.6% of Salt Typhoon's documented techniques. The remaining three classes, i.e., patch management (7.1%), cryptographic controls (7.1%), and threat intelligence (7.1%) each address three techniques. Notably, cryptographic controls at priority 6 target stored credential weaknesses (weak Cisco Type 7 passwords, offline brute-force attacks), not channel-layer protections.

Conspicuously absent: Quantum channel security. Under implementation-based assumptions, QS addresses 7.1% of techniques (3/42). Under implementation-agnostic assumptions, 21.4% (9/42). Operational controls (priorities 1–4, combined 78.6%) cover 11 times as many distinct techniques by count as cryptographic controls. Selective

[a]Monitoring, logging, anomaly detection, data loss prevention, and deep-packet inspection are treated as amplifiers of these structural controls rather than as a separate class. For example, egress monitoring is counted under network segmentation when it builds on and enforces egress policies, and behavioral analytics under access control when it evaluates the use of privileged actions. Borderline cases are resolved consistently with this principle.

quantum deployment on high-value links should follow, not precede, maturation of foundational controls.

This hierarchy reflects Salt Typhoon's threat model of on-device adversaries enjoying administrative access. Organizations facing passive HNDL threats should absolutely prioritize cryptographic modernization; those facing infrastructure-centric APTs, however, should focus on operational controls in the first instance. For most telecommunications operators, Salt Typhoon represents an especially salient threat model. Each dollar allocated to quantum infrastructure represents a dollar not spent on controls potentially yielding better security outcomes. No channel secured by quantum physics can protect a system patched seven years late.

Beyond Salt Typhoon: Generalizability to Infrastructure-Targeting Campaigns

Does the device-dominant pattern hold beyond Salt Typhoon? Examining other documented infrastructure-targeting campaigns suggests it does.

VPNFilter (2018)[10] infected at least hundreds of thousands of small office/home office (SOHO) routers and NAS devices across 54 countries. Its modular architecture enabled traffic inspection, credential harvesting, and destructive actions, all executed *from* compromised devices. Even VPNFilter's traffic-inspection and traffic-manipulation modules, including Modbus supervisory control and data acquisition monitoring and HTTP interception/injection, operated via device-resident code rather than passive channel interception. The campaign also appears to have exploited exposed and poorly secured devices, including ones with known public vulnerabilities or default credentials.

Cyclops Blink (2022),[11] Sandworm's successor to VPNFilter, targeted WatchGuard firewalls and other network devices with firmware-level persistence surviving reboots and the legitimate firmware update process. Its published MITRE ATT&CK mapping is overwhelmingly device-centric: firmware persistence (T1542.001), command-line execution (T1059.004), firewall modification (T1562.004), and C2 over TLS-protected web protocols initiated from compromised devices (T1071.001, T1573.002). All twelve documented techniques operate on the device.

Volt Typhoon (2021–present), attributed to PRC state-sponsored actors targeting U.S. critical infrastructure including energy, water, and transportation, mirrors Salt Typhoon's device-centric pattern despite targeting different sectors. Volt Typhoon compromises public-facing network appliances, uses living-off-the-land techniques predominantly (wmic, ntdsutil, netsh, PowerShell), moves laterally via valid credentials, and proxies traffic to targets through compromised SOHO and network edge devices. Its documented ATT&CK techniques concentrate overwhelmingly in credential access, discovery, lateral movement, and persistence,[15] all of which are device-level operations where channel-layer QS provides no meaningful defensive value.

The structural reason for this convergence is that campaigns targeting network infrastructure are operationally device-centric, even though network topology suggests a plethora of vulnerable channels. The operational value of infrastructure compromise lies in controlling devices that route, switch, and terminate traffic. An adversary operating from a compromised router can mirror, tunnel, and exfiltrate traffic regardless of the cryptographic protections applied to the channels between devices. Channel-layer attacks, such as passive interception in HNDL collection, represent a genuinely different threat model, one where the adversary sits *between* devices rather than *on* them. As such, they require different primary defensive investments. Our analysis of Salt Typhoon, corroborated by VPNFilter, Cyclops Blink, and Volt Typhoon, supports the expectation that device-centric compromise is common across several documented infrastructure-targeting campaigns.

Two further patterns strengthen the generalizability claim. First, these four campaigns span two independent nation-state adversaries, the PRC (Salt Typhoon, Volt Typhoon) and Russian GRU (VPNFilter, Cyclops Blink) and multiple strategic objectives, ranging from long-term espionage to prepositioning for potential disruption. Despite these differences in intent, both actors independently converged on device-centric tradecraft. This convergence suggests the pattern is driven by infrastructure architecture, not by any single adversary's playbook. Second, public reporting across these campaigns consistently points to heavy reliance on known vulnerabilities and other avoidable weaknesses for initial access. Across the cases, available patches, weak exposure management, and other governance failures repeatedly provided sufficient access. This recurring pattern across actors, target sectors and strategic objectives underscores that the limiting factor in infrastructure defense is not necessarily quantum-cryptographic strength but operational discipline, involving patch currency, access control, and configuration governance.

Our analysis of Salt Typhoon's 42 documented techniques shows that quantum security directly touches only 7%–21% of this APT campaign's attack surface. This is due to network architecture: quantum channel security protects *between* trusted devices,

while Salt Typhoon operated *from* compromised infrastructure that controlled encryption endpoints. In this campaign, operational controls, i.e., access control, configuration management, platform integrity, and network segmentation, address roughly 11 times as many distinct ATT&CK techniques by count than cryptographic controls.

This does not suggest QS is pointless; far from it. Forward secrecy protects past communications even if devices are compromised later, defending against HNDL adversaries with future quantum computers. QKD can raise adversary costs and provide tamper evidence, increasing operational complexity and detection risk. These forward-looking benefits are orthogonal to our retrospective analysis of Salt Typhoon's device-level operations. Organizations facing passive bulk collection on long-haul links have different priorities from those facing active infrastructure compromise; our findings speak to the latter threat model.

This distinction will only grow more urgent. As QS products mature and vendor advocacy intensifies, telecommunications operators will face increasing pressure to quantum-harden their networks. The logic will seem compelling as carrier networks contain vast numbers of channels, making them appear to be prime candidates for channel-layer cryptographic modernization. Our analysis serves as an early empirical corrective to this reasoning. The sheer number of channels in a telecommunications network does not automatically make channel-layer protection the priority when documented adversaries bypass those channels entirely by compromising the devices that terminate them. Without this evidence base, there is a risk that QS investment displaces the operational controls that would have materially degraded the campaigns actually observed in the wild.

More broadly, our analysis of the Salt Typhoon case illustrates a general approach to evaluating security technologies against real campaigns. Rather than starting from theoretical threat models or vendor promises, we start from what attackers actually did, classify where each technique is materially effective (channel or device), and see where a proposed technology can realistically degrade APT actions. The framework developed here can be used to compare emerging defensive technologies, from zero-trust architectures to hardware roots of trust and AI-driven anomaly detection, on the common ground of documented adversary behavior. In a parallel project, we are developing network-cascade models to quantify how infrastructure compromises propagate through layered telecommunications networks and how different defensive mixes constrain their scope.

Telecommunications operators face finite security budgets and a long shopping list of controls. Our analysis suggests that QS, while paramount for specific high-value links and long-term HNDL protection, should follow rather than precede investment in foundational operational hygiene. Salt Typhoon demonstrates that sophisticated APT actors exploit device-level weaknesses, governance gaps, and day-to-day operational failures. The unglamorous work of closing those gaps will remain critical, and no quantum fix can substitute for it. ■

Acknowledgment

Financial support from the Sam Nunn School of International Affairs at Georgia Tech and the Neal Family Endowment is gratefully acknowledged. The author thanks Rupal N. Mehta, Spenser A. Warren, and Nicolas Wittstock, as well as *IEEE Security & Privacy's* three anonymous reviewers and editors, for comments on earlier drafts. An anonymous independent expert validated the mapping scheme in a second round of coding. Claude (Anthropic) provided assistance with technical debugging of Python code and checking the consistency of quantitative claims. This article has supplementary downloadable material available at https://doi.org/10.1109/MSEC.2026.3688536, provided by the author.

References

1. "Countering Chinese state-sponsored actors compromise of networks worldwide to feed global espionage system," Joint Cybersecurity Advisory AA25-239A (U/OO/198904-25), Aug. 2025. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
2. T. Krásová, "2025 in review: Telecom gets entangled with quantum," *Light Reading*, Dec. 16, 2025. [Online]. Available: https://www.lightreading.com/security/2025-in-review-telecom-gets-entangled-with-quantum
3. U.S. House Committee on Oversight and Government Reform, Subcommittee on Military and Foreign Affairs, "Salt typhoon: Securing America's telecommunications from state-sponsored cyber attacks," Hearing, 119th Congress, Witnesses: E. Amoroso (TAG Infosphere/NYU), M. Blaze (Georgetown), J. Steinman (Galvanick), Apr. 2, 2025. [Online]. Available: https://www.congress.gov/event/119th-congress/house-event/118084
4. A. Goldman, "'Unrestrained' Chinese cyberattackers may have stolen data from almost every American," *The New York Times*, Sep. 4, 2025. [Online]. Available: https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html
5. A. Regenscheid, "Transition to post-quantum cryptography standards," Nat. Inst. of Standards and Technol., Gaithersburg, MD, USA, NIST IR 8547, 2024.
6. D. Shepardson, "Outgoing FCC head says salt typhoon hacking a clarion call to address security issues," *Reuters*,

Jan. 17, 2025. [Online]. Available: https://www.reuters.com/technology/cybersecurity/outgoing-fcc-head-says-salt-typhoon-hacking-clarion-call-address-security-issues-2025-01-17/

7. "Quantum-readiness: Migration to post-quantum cryptography," CISA, Arlington, VA, USA, Aug. 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
8. S. Rowley, "KETS quantum security reacts to salt typhoon cyber attacks," *Data Centre and Netw. News*, Jan. 10, 2025. [Online]. Available: https://dcnnmagazine.com/news/kets-quantum-security-reacts-to-salt-typhoon-cyber-attacks/
9. NCSC, "Quantum security technologies," White Paper, GCHQ, 2020. [Online]. Available: https://www.ncsc.gov.uk/sites/default/files/pdfs/publication/quantum-security-technologies.pdf
10. W. Largent, "New VPNFilter malware targets at least 500K networking devices worldwide," *Cisco Talos Blog*, May 23, 2018. [Online]. Available: https://blogs.cisco.com/security/talos/vpnfilter
11. "New sandworm malware cyclops blink replaces VPNFilter," *U.K. Nat. Cyber Secur. Centre*, Feb. 23, 2022. [Online]. Available: https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
12. "MITRE ATT&CK®." MITRE ATT&CK®. Accessed: May 4, 2026. [Online]. Available: https://attack.mitre.org/
13. "Security and privacy controls for information systems and organizations," NIST Special Publication 800-53, Revision 5, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
14. "Critical security controls." CIS Center for Internet Security. Accessed: May 4, 2026. [Online]. Available: https://www.cisecurity.org/controls
15. "PRC State-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure," Alert Code AA24-038A, Feb. 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Juljan Krause is an assistant professor of digital systems and international affairs at the Georgia Institute of Technology's Sam Nunn School, Atlanta, GA 30332 USA. His research interests include quantum computing and communications, internet technologies, and network theory. Krause earned his Ph.D. in computer science from the University of Southampton. He is a Member of IEEE. Contact him at jkrause@gatech.edu.