Salt Typhoon: A Historical Espionage Campaign

Cyber-Warfare: Actors, Techniques and Impact

Authored by: Amari (AJ) Jones

Instructor: Zachary Kelley

December 1, 2025

Executive Summary

In late 2024, a Chinese state-sponsored hacking group known as “Salt Typhoon” executed a sweeping cyber-espionage campaign targeting United States telecommunications networking and dozens of others globally. Attributed to China’s Ministry of State Security, the operation exploited a zero-day vulnerability in Versa Networks’ SD-WAN platform (CVE-2024-39717) and unpatched flaws in Cisco and Fortinet devices, enabling covert access to core network infrastructure for 12-24 months (Madhani, 2024).

In contrast to conventional endpoint breaches, Salt Typhoon specifically targeted network management equipment and backbone routers, which are often unmonitored. The attackers gained access to law enforcement surveillance logs, collected call metadata, and intercepted high-profile people’s voice conversations, including those of United States officials (Nakashima, 2024). Millions of messages were unintentionally exposed, even though less than 150 targets were directly hacked.

United States authorities noted that this breach ever surpassed SolarWinds incident in breadth and sensitivity, making it one of the most destructive espionage breaches in United States infrastructure history. Systemic telecom security flaws such as outdated gear, a lack of MFA, and blind spots in network-level visibility, were brought to light by this campaign.

The federal response was swift. Agencies like the FBI, CISA, and NSA issued emergency directives, and President Biden prioritized telecom security with high level briefing and policy review. In the aftermath, the United States pushed for new regulations and further restricted Chinese telecom tech access.

This report analyzes the Salt Typhoon campaign and its strategic context, technical execution, and lasting implications for cybersecurity policy and critical infrastructure defense.

Introduction

The purpose of this report is to analyze and provide a case study of the late-2024 Salt Typhoon cyber warfare/espionage incident that targeted telecommunication providers. The goal of this is to understand the incident's objective, techniques, and consequences within a broader scope. By dissecting this case using different methodologies, the aim is to illustrate how state-sponsored threat actors use long-term espionage campaigns against critical infrastructures. This incident was selected because of its recency and is described as *"the worst telecom hack in our nation's history*" nationwide (Nakashima, 2024), making it an ideal case to explore the tactics and impact involved.

The report is sourced from different methodologies, drawing on open-source intelligence (OSINT) from government statements, news reports, and technical analyses. The information that is key to this report was gathered from credible sources like Reuters, The Washington Post, Associated Press, and other official advisories and intelligence blogs. For this report, the MITRE ATT&CK framework is used to map the threat actor's tactics and techniques. The Lockheed Martin Cyber Kill Chain model guides the step-by-step breakdown of the operation, and the Diamond Model provides a view of the adversary, infrastructure, capabilities, and victims.

Historical Context

Social Environment

The Salt Typhoon espionage operation emerged during a time of deep digital dependence. By 2024, mobile and internet services were embedded in nearly every aspect of our lives in America, making the breach potentially far-reaching. Awareness of cyber threats was increasing, yet many still assumed basic telecom services were secure. The breach occurred just before the 2024 United States presidential election, amplifying concern even though officials said it was not election related (Nakashima, 2024), reports that Chinese hackers accessed communications tied to candidates like Donald Trump and Kamala Harris drew alarm. Nevertheless, the incident did strike tension amidst U.S. and China relation with skepticism towards Chinese tech and products like TikTok already growing.

Economic Environment

The telecom sector in 2024 was marked by advanced services layered over aging infrastructure of core equipment more than 12 years old. Major carriers like AT&T, Verizon, T-Mobile, and Lumen operated on networks cobbled together through decades of mergers, often relying on outdated, un-patchable equipment (Nakashima, 2024). Budget constraints contributed to delayed modernization and uneven cybersecurity. Economically, the breach imposed a direct cost including incident response, forensic audit, system patches, and potentially large scale hardware replacements. Concerns also exist that the hackers may have targeted corporate IP and sensitive communication to benefit Chinese state-linked enterprises.

Technological Environment

By the mid-2020s, networks were highly connected but often insecure at the infrastructure level. Critical sectors relied on digital and remote management, increasing exposure to reconnaissance. While tools like encryption, multi-factor authentication (MFA), and intrusion detection systems (IDS) were widely available, implementation gaps persisted. Salt Typhoon exploited these gaps, targeting nontraditional IT components like routers and leveraging a zero-day in Versa Director (Lumen Technologies, 2025) and known flaws in the Fortinet and Cisco devices (Wikipedia contributors, 2025). Poor “cyber hygiene” was the critical factor that played into this as one major victim lacked MFA on an admin account, granting control over tens of thousands of routers. This operation reflected an evolution in APT tactics, leveraging overlooked infrastructure with stealth tools like fileless malware and custom web shells.

Geopolitical Climate

This hack occurred during the escalating cyber rivalry between both the U.S. and China. The U.S. had labelled the Chinese APTs as an “epoch-defining threat” (Page, 2025), this is a reflection of how espionage campaigns increasingly focused on prepositioning within critical infrastructure. Campaigns like Volt Typhoon (targeting Guam’s power grid), Flax Typhoon (targeting IoT Devices) were part of this pattern, illustrating Beijing’s long-term prepositioning strategy. Salt Typhoon fits into this broader category of persistent, preparatory intrusion.

Meanwhile, the global environment saw cyber operations becoming a key tool in modern statecraft. Russia’s cyberattacks during its Ukraine invasions reinforced military relevance of digital operations. Within the climate, China’s intrusion into the telecoms served dual aim: collect intelligence and preposition disruption capabilities. It unfolded as Washington imposed tighter tech sanctions on China, prompting Beijing’s predictable denials and counteraccusations (Madhani, 2024).

Actors Involved

Primary Adversary (Threat Actor A).

The Perpetrator of this campaign is an advanced persistent threat (APT) group attributed with the Chinese state, publicly known and codenamed as "Salt Typhoon." Investigators linked them to China's intelligence, specifically the Ministry of State Security (Wikipedia contributors, 2025). In terms of actor type, it is a state-sponsored espionage unit, not cybercriminals or hacktivists.

The group's motivations are predominantly geopolitical and strategic, conducting cyber-espionage to collect intelligence on foreign governments, military, and other targets of interest in order to bolster China's strategic positioning (Page, 2025). There may also be economic espionage as a secondary motive (stealing corporate data or IP), lining with the hacking patterns. Regarding capabilities, Salt Typhoon represents a top tier threat actor with significant resources and sophistication, demonstrating the ability to acquire zero-day exploitations, and carry it out in long term.

Known operations by Chinese APTs related to Salt Typhoon provide context as noted to "Volt Typhoon" is closely related group that infiltrated power and communications infrastructure in years prior (Page, 2025). Likewise, Hafnium (later codenamed "Silk Typhoon") hacked Microsoft Exchange servers in 2021 (Page, 2025). Salt Typhoon appear to be part of this continuum of Chinese cyber units "gearing up for war" by gathering information and establishing footing in critical systems. Meanwhile, their sponsorship links are clear, attributing to a nation-state, and the tactic of espionage align with Chinese government interests.

Secondary Actor or Opposing Entity

The primary defenders were U.S. telecom providers like AT&T, Verizon, T-Mobile, Lumen, and federal cybersecurity agencies. Initially caught off guard, these companies had varied cybersecurity maturity with some lacking adequate network monitoring (Page, 2025). Once alerted, the U.S. response mobilized through CISA, NSA, and the FBI, coordinated by the National Security Council. Using frameworks like MITRE ATT&CK, defenders analyzed the breach and deployed incident response teams. However, readiness was poor. Senator Mark Warner highlighted the telecom industry's lax regulatory oversight and prevalence of legacy vulnerabilities (Nakashima, 2024). Although response efforts scaled rapidly by late 2024, the incident revealed the need for stronger regulation and preparedness (Madhani, 2024).

Non-State Entities

Key non-state actors included private security firms and affected individuals. Microsoft Threat Intelligence Center and Lumen's Black Lotus Labs uncovered the intrusion and Versa Director zero-day exploits (Microsoft initially flagged unusual activity, and Lumen specifically uncovered the exploit) (Lumen Technologies, 2025). These firms shared indicators of compromise with telecoms and federal agencies. Allies from Five Eyes nation also co-signed advisories and shared intelligence.

On the adversary side, the use of contractors or front companies which are common in Chinese APT campaigns remain a possibility. For instance, Flax Typhoon reportedly used a Beijing-based security firm to mask operations (Page, 2025). But as it stands right now, it's not confirmed for Salt Typhoon.

Stakeholders / Victims

Primary victims were major telecom and ISPs, which are core elements of critical infrastructure. At least 8-9 carriers were affected, along with providers in roughly two dozen other countries. In the United States, communications from government agencies (Congress, Military, White House, etc.) were targeted, including phones tied to a former President and Vice President campaign team (Nakashima, 2024).

Roughly 150 direct victims (primarily government officials in D.C.) had their communications surveilled, while many more were swept up via contact metadata, impacting public trust. Strategically, the access allowed China to monitor United States law enforcement efforts through the wiretapping systems, identifying Chinese agents under surveillance. The carriers themselves were high-value targets. Compromising them enabled lateral access to downstream networks and users. Finally, the stakeholders ranged from telecoms and government agencies to affected civilians and international allies. By undermining secure communications, Salt Typhoon threatened the foundation of national security and civil trust in digital systems.

Cyber Operation Overview

Timeline of Events

The Salt Typhoon espionage campaign spanned out in multiple phases over at least two years of 2023 to 2025 (*Salt Typhoon | NJCCIC*, n.d.).

- **Mid-2023 (or earlier):** Chinese attackers likely began reconnaissance and initial infiltrations. Officials believe the hackers had been in some networks "at least a year or two" before discovery (Madhani, 2024). By early 2024, the adversary had already gotten

into networking devices in several telecommunication companies, prresumably through existing known exploits.

- **June 2024**: There was an active zero-day exploitation in Versa Network's director software. Black Lotus Labs recorded that on June 12th, 2024 threat actors used a custom web shell known as "VersaMem" to exploit Versa Director servers at multiple managed service providers, suggesting that by June 2024, the attackers were accessing using the newly discovered CVE-2024-39717 (Lumen Technologies, 2025).
- **August 2024:** The campaign quietly continued. Versa Networks announced the SD-WAN Director vulnerability and patch on August 22nd, 2024 (Lumen Technologies, 2025). A few days later, on August 27th, 2024, The Washington Post posted the story that at least two major U.S. internet providers were compromised by Chinese hackers (Wikipedia contributors, 2025). The same day, Lumen's threat team published details on the Versa Director zero-day exploitation (Lumen Technologies, 2025). These were the first public alarms, though the full scope was not yet known.
- **Late September 2024**: The United States government became fully engaged. By Warner's account, "late September" was when federal agencies grasped the seriousness of the breach (Nakashima, 2024). This indicates that telecom companies and possibly Microsoft had by then escalated their findings to the government. Around that time, hunting guides and indicators of compromise were shared with major telecom providers to help them flush out the hackers (Wikipedia contributors, 2025).
- **Early October 2024**: More details emerged. On October 5th, 2024, news broke out that Chinese hackers had even accessed United States wiretap systems used for lawful intercepts (Wikipedia contributors, 2025). On October 6th, 2024, Washington Post reported intrusion in multiple U.S. Telecoms, calling it an apparent Chinese counter-spy operation. By October 25, media reported Salt Typhoon has targeted phones of high-profile politicians. Meanwhile, telecoms began remediation quietly.
- **November 2024**: Recognition of the hack's scale led to policy attention. On November 21st, 2024, Senate Intelligence Chair, Mark Warner, publicly labelled it the worst telecom hack in the U.S. history (Nakashima, 2024). He showcased new insights (real-time call listening, multi-network spread) and warned that hackers remained in the network (Nakashima, 2024). By late November, at least 8 United States telecom companies and approximately 24 countries were understood to be affected (Madhani, 2024).
- **December 2024**: Official response kicked into high gear. On December 4th, 2024, a senior White House official named Anne Neuberger publicly disclosed that "a large number of Americans' metadata was taken" in this campaign (Satter, 2024). The FBI, CISA, NSA, and international partners released joint guidance on securing telecom networks on December 5th (*Salminen & Kotfica, 2024*). By mid-December, the Biden Administration took initial retaliatory steps such as issuing notice against China Telecom's U.S. subsidiary as a national security threat (first reported December 16th) (Escobedo, 2024). On December 27th, 2024, the White House confirmed a ninth U.S.

telecom was found breached after further hunting and emphasized ongoing efforts to pursue the hackers (Wikipedia contributors, 2025). At the end of the year, some companies like (AT&T, Verizon, and Lumen) have announced they had eradicated the threat from their networks (Page, 2025).

- **Early 2025**: Continued aftermath and disclosure. In January 2025, more details came out on how Salt Typhoon conducted their campaign and this information possibly dated back to early 2024, or late 2023. The U.S. Treasury was also hacked by "Silk Typhoon", showing simultaneous Chinese campaigns (Page, 2025). By this time, the bulk of Salt Typhoon's access was removed, though assessment on the damages continues.

In summary, the initial compromise happened quietly well before mid-2024, but exposure happened in the third quarter of that year. Remediation started in the fourth quarter of the year and by early 2025, the incident was largely contained. They also might have had a secondary objective of gathering corporate data or tech secrets whilst traversing the networks.

Attack Objectives

Salt Typhoon's objectives were firmly in the realm of espionage and intelligence collection, rather than disruption or destruction. With this, they had achieved and maintained a foothold in critical infrastructure for future exploitation.

The primary goal was clearly to intercept sensitive communications of U.S. persons of interests. By accessing telecom networks and databases, the attacker obtained call detail records and text message meta data at scale. The metadata (who called whom, when, and from where) can reveal social networks and patterns of life for intelligence targets. In some instances, Salt Typhoon could capture audio of phone calls if they were not end-to-end encrypted. Essentially, the attacker sought to listen in by using Man-In-The-Middle methods to access conversations of United States government officials, politicians, and possibly high value individuals.

Another troubling objective was accessing law enforcement wiretapping systems. The hacker compromised systems used for court authorized data collection. By doing so, they learned which phone number and accounts U.S. agencies were targeting. The goal here was likely to identify Chinese agents or assets under investigation and tip off Chinese Authorities. CBS News summarized that there was fear the hack let China discover "information about ongoing United States Investigation, including those tied to China" (Escobedo, 2024).

Another objective was to have a foothold in critical infrastructure for potential future exploitation. Even though Salt Typhoon did not sabotage or disrupt during 2024, by implanting themselves in telecom networks, they were positioned to do so if desired. This aligned with China's broader goal of "preparing the battlefield" in case of a future conflict.

Lastly, the secondary objective was to obtain corporate data and tech secrets. Salt Typhoon had time to traverse the networks including on a corporate and enterprise level, also being seen in reports have searched for corporate intellectual property on targeted networks (Salminen & Kotfica, 2024).

There's no indication of financial gain/ransom or influence operations/propaganda being the objective. Nor was it aimed at destroying the infrastructure due to the hackers being careful to remain undetected to prolong the espionage. In summary, this campaign was espionage-centric to quietly obtain as much sensitive communications as possible while staying persistent with their access for China's intelligence.

Scope and Scale

The scope of Salt Typhoon's operation was extensive and international, affecting dozens of countries across multiple continents, but with deep focus in the United States (Madhani, 2024). Within the United States, at least 8 major telecom firms were compromised, which ultimately compromised a large portion of the country's phone and internet backbone (Satter, 2024). The campaign's reach extended to potentially over a million end-user devices or accounts whose metadata was collected.

The scope also includes multi-domain impact from telephones (intercepting voice calls), messaging (texts/SMS metadata were stolen), and network operations. The supply chain aspect was notable too, hitting a common software used by many internet service providers. They leveraged one vulnerability to pivot several environments (Lumen Technologies, 2025). Salt Typhoon also showed that it can go between organizations, exploiting inter-carrier connections and trust relationships to expand the breach.

In summary, the campaign was massive in scale and attacked at a nationwide level, especially in the United States, and multi-national globally, touching potentially millions of individuals' data. The breach was also colossal in scope by some measures, perhaps the largest compromise of telecom network ever publicly reported, making it a landmark case in cyber-espionage scale and complexity.

Technical Analysis

Threat Actor Profile

Salt Typhoon is a classified nation-state Advanced Persistent Threat (APT) group, attributed to Chinese Ministry of State Security (MSS). Their tactic, technique, and procedure (TTPs) are consistent with a highly sophisticated espionage group. Key TTP characteristics include:

- **Initial Exploitation of Network Appliances:** Rather than typical phishing or endpoint malware, Salt Typhoon distinguished itself by exploiting internet-facing network devices. They leveraged at least one Zero-Day Exploit in Versa Director SD-WAN management software (Lumen Technologies, 2025), deploying a bespoke web shell ("VersaMem") to capture credentials and run code in the memory. They also took advantage of unpatched and legacy Cisco and Fortinet routers. This operation of targeting routers/VPNs aligned with what Microsoft observed in Volt Typhoon's campaign in the mid-2020s. It suggests a preference for network infrastructure as an entry vector.
- **Stealth and Living-off-the-Land:** Once inside, Salt Typhoon operated quietly to avoid detection. They used legitimate credentials (stolen via webshell) to masquerade as a normal admin (Lumen Technologies, 2025). They avoided deploying noisy malware instead they likely implanted rootkits or backdoors on the firmware (Harris, 2025). They also exploited trusted network links like using their foothold in one telecom to move laterally into interconnected networks, essentially riding the "trusted traffic" between providers (Nakashima, 2024).
- **Command-and-Control (C2) Infrastructure:** The attacker's C2 infrastructure likely involved compromised devices and proxies. Chinese actors often use "hop points" on small-office/home-office (SOHO) routers or servers globally to route traffic. This infrastructure obfuscated attribution and allowed attackers to perform long-term data theft campaigns. In some cases, they reconfigured compromised routers to exfiltrate data directly to attacker-controlled destinations.
- **Toolset:** The VersaMem webshell was a key component, designed to intercept credentials and allow in-memory execution of attacker code on the SD-WAN platform. They may have also used variants of known Chinese malware for network gear. Some reporting suggest they had implants to monitor voice traffic and metadata databases. Standard networking tools like telnet/SSH clients and network configuration commands were abused as well. No ransomware or destructive malware was used.
- **Attribute Confidence:** Attribution to China is considered highly reliable. Analysts from Microsoft, Secureworks, and United States intelligence agencies noted significant overlap

between Salt Typhoon and previous Chinese APT campaigns like Volt Typhoon Hafnium (Silk Typhoon), including shared TTPs, infrastructure, and strategic targets being network infrastructures (Lumen Technologies, 2025). The U.S. government publicly linked the group to China's MS, citing both technical and strategic indicators. The scope of the campaign and nature of the intelligence collected strongly align with the Chinese geopolitical priorities, especially in the context of strategic competition with the United States.

MITRE ATT&CK Mapping

Salt Typhoon's method maps comprehensively across the **MITRE ATT&**CK matrix, illustrating a full-spectrum staged espionage campaign:

- **Initial Access (T1190):** Exploited vulnerable internet-facing systems, including Versa SD-WAN and Cisco/Fortinet Devices. (MITRE Technique T1190 – Exploit Public Facing Application) (Lumen Technologies, 2025).
- **Execution (T1505, T1059):** Leveraged webshells (MITRE Technique T1505 – Server Software Component) and command-line interfaces on routers (MITRE Technique T1059 – Command and Scripting Interpreter).
- **Persistence (T1542.003, T1505, T1078):** Used system firmware implants (T1542.003 – Pre-OS Boot: Bootkit, Sub-technique), webshell backdoor (T1505 again), and valid accounts for long-term access (T1078 – Valid Accounts).
- **Privilege Escalation (T1068):** Abused credentials to gain administrative access, particularly where MFA was absent (T1068 – Exploitation for Privilege Escalation).
- **Defense Evasion (T1562, T1027, T1078, T1090):** Salt Typhoon employed numerous evasion techniques. Disable or Modifying Tools (T1562 – Impair Defenses) might apply if they turned off logging or security features on network devices. Obfuscated files or information (T1027 – Obfuscated Files or Information); their webshell was disguised as a .png file and had zero antivirus detections when uploaded to VirusTotal (Lumen Technologies, 2025). They also used Valid Accounts (T1078 – Valid Accounts) to blend in and likely Multi-hop Proxies (T1090 – Proxy) using intermediate nodes to mask origin. Additionally using living-off-the-land allowed them to avoid running suspicious processes (T1560 – Archive Collected Data).
- **Credential Access (T1056, T1557, T1003):** Captured credentials using web shells (T1056 – Input Capture), intercepted authentication flows (T1557 – Adversary-In-The-Middle), and dumped router configurations (T1003 – OS Credential Dumping).
- **Discovery (T1590, T1016, T1012):** Mapped out network infrastructure and interconnections (T1590 – Gather Victim Network Information) for listing routing tables, connected networks and trusted links. On servers, it might run a configuration to see how networks are segmented (T1016 – System Network Configuration Discovery). Lastly

they more than likely have performed querying on identified data repositories (T1012 – Query Registry) to find specific targets.

- **Lateral Movements (T1210, T1090.001)**: Salt Typhoon excelled at lateral movements. They used Exploitation of Remote Services (T1210 – Exploitation of Remote Services) by using stolen credentials to log into additional routers, switches, or servers within and across networks. They also possibly used Internal Proxy (T1090.001 – Internal Proxy) techniques, routing through one compromised device to access others. The ability to "move from one telecom network to another, exploiting relationships of trust" is explicitly noted. Within a single provider, lateral movements would include hopping from an SD-WAN controller to customer edge devices or from core routers to monitoring system.
- **Collection (T1114.003, T1040)**: The attackers were laser-focused on collecting communications data. They accessed call detail record databases which contained metadata like numbers, timestamps, cell tower info, etc (T1114.003 – Email and Phone Number Harvesting). They also collected SMS/text message metadata and content (Page, 2025). Importantly, they were able to collect audio intercepts for certain calls. This implies Network Sniffing (T1040 – Network Sniffing) or hooking into VoIP streams.
- **Exfiltration (T1048, T1022, T1041)**: To exfiltrate the stolen data back to themselves, Salt Typhoon employed a few clever techniques. They reconfigured Cisco routers to forward data out of the network to external servers (Nakashima, 2024), using Exfiltration Over Alternative Protocol (T1048 – Exfiltration Over Alternative Protocol). Given the volume of data, they likely did it in batches over encrypted channels (T1022 – Data Encrypted). They might have piggybacked on an existing VPN tunnel or created new tunnels from compromised devices to attacker infrastructure (T1041 – Exfiltration over C2 Channel).
- **Impact (T0882):** Primary effects was the theft of confidential data (T0882 – Data Breach), with potential for future disruption though no availability or integrity attacks were observed.

Kill Chain Analysis

Using **Lockheed Martin Cyber Kill Chain** model, the operation unfolded as follows:

- **Reconnaissance:** Identified telecom providers running Versa SD-WAN and unpatched software through internet scanning, open-source intelligence, and service fingerprinting.
- **Weaponization:** Developed or acquired the Versa zero-day and embedded it into a disguised payload (VersaMem).
- **Delivery:** Sent crafted HTTP requests to public management interfaces; possibly pushed malicious configuration downstream via compromised SD-WAN controllers.

- **Exploitation:** Remotely executed code on vulnerable devices to gain administrative access, especially in systems lacking MFA.
- **Installation:** Deployed web shells, rootkits, and possibly custom firmware modifications to enable persistence and collection.
- **Command & Control (C2):** Maintained access to multi-layered C2 infrastructure using hijacked SOHO routers and encrypted proxy channels.
- **Action on Objective:** Collected and exfiltrated sensitive communication data, including audio intercepts, call metadata, and surveillance logs, and remain active for as long as possible (Nakashima, 2024).

Notably, the installation phase (deployment of backdoor protocols) went unnoticed due to lack of firmware integrity monitoring that is an oversight and failure point in telecom defenses. Earlier in the chain, more robust network anomaly detection during the Delivery phase might have alerted a defender.

Diamond Model Analysis

The **Diamond Model** provides a relational framework to understand Salt Typhoon's campaign through four interconnected elements:

- **Adversary:** A Chinese APT team linked to the MSS, with long-term espionage objectives aimed to the United States Government and infrastructure targets (Page, 2025). Their risk calculus permitted high-impact intrusions due to the value of intelligence obtained.
- **Capabilities**:
    - *Exploits*: Zero-Day Exploits to Versa Director (CVE-2024-39717), exploit for known router vulnerabilities.
    - *Tools*: VersaMem web shell, firmware implants, covert network sniffing tools.
    - *Techniques*: Credential theft (harvesting login credentials to pivot); network reconnaissance and lateral movements across trust boundaries, data exfiltration via covert channels.
    - *Resources*: C2 infrastructure of proxy nodes (compromised SOHO devices used in attacks).
    - *Knowledge*: Deep understanding of telecom systems and lawful intercept technology, indicating possibly insider knowledge or extensive research.
- **Infrastructure**:
    - The infrastructure used included attacker-operated servers and compromised SOHO routers functioning as relay points, plus trusted inter-carrier connections exploited for stealth lateral movements. For example, attacker-operated servers that received exfiltrated data (likely hosted in China or bulletproof hosting locations). Also, the "hop points" like compromised routers outside the victim

space. Additionally, the victim's infrastructure were the network Salt Typhoon became apart of by performing their espionage campaign.

- **Victim:**
    - **Organizational**: AT&T, Verizon, T-Mobile, Lumen, and other high value interconnected telecoms operating legacy infrastructure.
    - **Individual**: Senior United States officials, law enforcement, campaign personnel, and international counterparts.
    - **Systemic**: FBI Surveillance records and lawful intercept logs, which may have compromised ongoing investigations.

These elements interlocked to form a highly coordinated espionage campaign. Salt Typhoon used its capabilities to weaponize infrastructure, exploit victim vulnerabilities, and extract high-value intelligence while remaining undetected for more than a year.

Impact Assessment

Operational Impact

Operationally, the campaign caused no immediate disruptions as calls and data continued to flow normally. This was a stealth operation and it was done so with intention, allowing the attackers to maintain covert access. However, discovery triggered a large scale operational response, having telecom providers isolate systems, patch vulnerabilities, and possibly replace hardware. Including 5,000-15,000 devices as Senator Warner noted (Nakashima, 2024).

For the U.S. government, the breach impacted counterintelligence and secure communications. Agencies feared sensitive calls were monitored, prompting shifts to encrypted messaging and secure systems as recommended by CISA (Salminen & Kotfica, 2024). Cybersecurity agencies like the FBI, NSA, and again, CISA, diverted resources to assist affected networks, slowing other priorities.

Importantly, the breach exposed latent operational risks, had it gone undetected, China could've sabotaged networks in a crisis. Though that scenario didn't materialize, the threat forced officials to confront how deeply core systems can be compromised without visible effects.

Strategic or Geopolitical Impact

This hack had significant strategic and geopolitical ramifications, especially for the United States and China's relation. It marked a major counterintelligence breach for the United States, exposing sensitive telecommunication infrastructure and prompting swift retaliation. The

United States responded with sanctions and actions against China entities like China Telecom (Escobedo, 2024), intensifying diplomatic tension as China denied involvement and issued counteraccusations (Madhani, 2024).

Strategically, this reinforced the United States' fears that China is pre-positioning within global infrastructure for potential future conflict scenarios (Page, 2025). Lawmakers pushed for a more offensive posture, signaling a possible shift in the direction of a proactive cyber operation. From China's perspective, the operation may have yielded strategic intelligence, potentially informing their foreign policy and counter-intelligence efforts. However, this came at the cost of international backlash.

Economic Impact

While espionage-focused cyber operations like this one don't cause immediate financial losses like ransomware attacks, they generate a substantial economic impact. For affected telecom companies, direct cost includes hiring incident response teams, conducting forensic audits, deploying patches, and possibly replacing thousands of compromised routers and switches. Though companies like T-Mobile downplayed customer impact, public relations and notification efforts still incurred costs (Satter, 2024).

Reputation damage also played a role in the situation. Even if consumer churn is low due to limited alternatives, trust erosion among enterprise and government clients can lead to contract hesitation or increase compliance demands. The FCC proposed certification rules (Salminen & Kotfica, 2024) may require expensive infrastructure upgrades and operational changes, adding to long term compliance costs.

Any stolen IPs or business communications could have economic consequences. If Salt Typhoon accessed sensitive R&D or negotiation data, that intelligence loss might benefit foreign competitors and cost affected companies' well above $50 million collectively, encompassing incident response, auditing, and hardware turnover. Unfortunately, agencies like the FBI reflected another layer of the economic impact as investigative cost incurred to public resources. While less visible than a destructive attack, this attack had a underscoring financial toll.

Social & Psychological Impact

The Salt Typhoon espionage campaign had a significant social and psychological impact which was centered on trust and perception. For the American public, learning that Chinese spies infiltrated core telephone networks was jarring and could erode confidence in our everyday communication. A common adage was that 'they could be listening', which could have been easily dismissed as paranoia, but it became a justifiable fear after this breach. The public learned that a foreign actor truly could be intercepting private calls in real time, shattering assumptions

of privacy. People generally assumed that their metadata were private except for the law but even then it's by court order, but this hack shattered that illusion by showing that a foreign actor can be listening in on audio calls in real time in some cases (Nakashima, 2024).

The hack has also likely intensified public suspicions towards China. In recent years, Americans have grown more mindful of cyber threats from nation-states and a highly publicized breach of telecom providers by China reinforces negative perception and could have social ramifications from reduced trade and business cooperation to a rise in xenophobic sentiment. This hack also validates concerns that has been raised about Chinese tech (like why Huawei was banned).

Another social impact is on employees and leadership of the victim companies. Internally, knowing one's company was utilized to spy on millions can hurt morale and pride. There could be blames and finger-pointing, especially towards the Information Technology teams and CEO, pushing for a cultural change within the organizations to prioritize security.

On the positive side, awareness of this breach may have some constructive social impact by increasing cybersecurity awareness. If people become more aware that SMS and standard calls aren't secured fully, they might adopt secure messaging for sensitive conversations.

On a transnational social impact, countries like Ukraine, which had seen Russian's cyberattacks, hearing that the United States was too hit by China might foster a sense that "no one is safe," but also solidarity in the need to combat cyber aggression.

In summary, socially and psychologically, the Salt Typhoon hack has heightened paranoia and vigilance. The public's distrust rose sharply, as Reuter surveys showed 70-80% public concern over foreign cyber intrusion. It more than likely has diminished some public trust in the security of essential services and infrastructure but also educated stakeholders to improve defenses.

Defensive Posture & Response

Immediate Responses

Once the intrusion was discovered and its scope became apparent, a **multi-layered incident response** kicked in. Containment and eradication efforts began with compromised telecom companies in close coordination with the United States government cyber teams. A key immediate step was the FBI and CISA indicators of compromise (IOCs) and a detailed "hunting guide" to telecom providers as mentioned before so they could scan their networks for hacker's presence.

In hand with that, incident response teams worked to **disconnect or patch** vulnerable systems, for example applying the Versa Director software patch released in August 2024 (Lumen Technologies, 2025) and upgrading to Cisco/Fortinet devices to remove known exploits. Where the bad actor's web shells or backdoor accounts were found, they were immediately removed. However, completely removing Salt Typhoon proved to be challenging. As of early December, Anne Neuberger noted that none of the affected companies had fully removed the Chinese actors from these networks (Madhani, 2024), yet implying ongoing efforts.

Communication and transparency were also part of the immediate response. The White House took an unusually public stance for an espionage act by holding press calls and briefings to inform the public and stakeholders about the breach (Madhani, 2024). The disclosure was aiming to raise awareness and also serve as a deterrent message to China that the United States knew what happened. There was also a briefing among officials from the FBI, NSA, DNI, FCC and more to inform lawmakers of the situation to ensure political leaders were in the loop and like bring the support for the response measures (Satter, 2024).

On the **technical guidance** front, immediate advisories were released. Joint cybersecurity advisories from the FBI, CISA, NSA, and other agencies came out outlining the nature of the threat and best practices to mitigate it along with a hunting guide. This also allowed companies to increase logging and monitoring of the network devices, applying available patches to commonly targeted gear, and implement out-of-band network management to detect anomalies (Salminen & Kotfica, 2024). The absence of centralized firmware logging, weak MFA enforcement, and lack of lateral-movement detection were the three core detection failures.

Long-Term Cybersecurity Measures

In the wake of the incident, numerous longer-term measures and reforms were proposed or implemented to bolster the security in telecom sectors. One significant measure came from the FCC. In December 2024, the FCC proposed a Declaratory Ruling, affirming that under existing law, telecom carriers are legally obligated to secure their networks against unauthorized access. In hand with this, the FCC published a Notice of Proposed Rulemaking where telecommunications providers must make an annual attestation to certify that they have a proper risk management plan in place. If this is adopted, it would take effect immediately (Salminen & Kotfica, 2024). This breach demonstrated that router-level monitoring cannot be optional. MFA on an administrative access *must* be mandatory across all carriers, and inter-provider peering trust must be actively policed.

In hand with this, the CISA, FBI, NSA, and government partners from Australia, Canada, and New Zealand co-signed an interagency guidance offering the information security team of communications infrastructure a list of practices to "strengthen their visibility and harden their network devices against successful exploitation." (Salminen & Kotfica, 2024). The guidance

emphasized improvements such as monitoring for lateral movements across routers, segmenting internal networks, and disabling unused remote tools.

At the industry level, major telecom firms began internal reforms: deploying red teams focused on network hardware, enforcing multi-factor authentication on admin accounts, and increasing broad-level oversight.

In this time, there were some crucial lessons for both the public and private sectors in cybersecurity. One major example was the strength, the public and private sectors learned to collaborate once the threat was recognized. Microsoft and Lumen's detection efforts that was paired with swift cooperations from federal agencies were crucial in identifying the threat and attributing it quickly (Lumen Technologies, 2025). The White House's prioritization ensured that the response was cross-agency and coordinated rather then siloed (Madhani, 2024). The weakness that was exposed was the breach also revealed critical deficiencies. A major failure was the use of privileged accounts without MFA (Wikipedia contributors, 2025), a basic security control that could have blocked initial access. Visibility into network infrastructure was another issue that many providers lacked. With the lack of proper monitoring of routers and switches, threatening them as passive elements, this blind spot allowed attackers to dwell undetected.

The espionage campaign served as a reminder of the importance of foundational practices like monitoring, patching and the use of multi-factor authentication, along with coordinated intelligence sharing and regulatory reporting. This also underscores that far more mandatory standards are needed to ensure that security is upheld and maintained. Going forward, the case will likely influence reforms across telecoms and other critical infrastructure sectors globally.

Ethical, Legal, and Policy Considerations

International Law and Norms

The espionage operation rases important issues on a legal and a normative standpoint. From the United States' perspective, the intrusion into our network is arguably a breach if sovereignty. While nothing physical occurred, international law doesn't clearly prohibit espionage, making it legally ambiguous. The 2015 UN GGE norms advised against targeting infrastructure during peacetime. Though Salt Typhoon didn't cause any outages, compromising telecom infrastructure and accessing law enforcement technology could be seen as a violation in light of the norms.

Due to the lack of a retaliatory action, the act likely falls short of the threshold of unlawful intervention or armed attack under the international law. No coercion or use of force was observed, the U.S. responded with non-military tools like sanctions and public attribution,

framing it as espionage rather than an act of war. According to Tallinn Manual, espionage itself is not illegal under international law, but it's method if violating sovereignty or norms can be. This may fuel calls to extend cyber norms to include intrusion into critical systems, even when nondestructive.

Ethical Issues

Ethically, Salt Typhoon raised serious concerns. The bulk surveillance of millions of people, including those with no intelligence values constituted a violation of their privacy rights (Nakashima, 2024). This mirrors earlier debates on mass surveillance but without any legal oversight or justifications from the collecting state. Exploiting a zero-day in Versa's systems before its disclosure also raises ethical concerns, as it left many global users vulnerable. While states argue nation security needs, withholding such vulnerabilities undermines global cyber safety.

How the United States responded also contained ethical dilemmas. Some officials floated retaliatory cyber operations (Escobedo, 2024), which introduces risk of collateral damage and escalation. Ethical countermeasures must uphold proportionality and avoid causing undue collateral damage or escalation into a cyber war. There's also risks to individuals under U.S. lawful surveillance. If Chinese operations identified targets, consequences could include retaliation or harm, especially in the case of dissident or activists. The burden thus extends beyond data theft to human consequence.

Policy Implications

Salt Typhoon has major implications for cyber policies. In the United States, it accelerated moves to regulate telecom as critical infrastructure, like sectors like energy or finance. The FCC's proposed attestation rules (Salminen & Kotfica, 2024) represents a move from voluntary best practices towards enforceable requirements, a standard. It may also prompt legal revision to mandate encryption and data protection.

The incident strengthens arguments to identify high-risk entities and enhancing oversight.. It reinforces the need for clear reporting timeline as delay in disclosure can create friction in coordination between agencies like the NSA and telecom firms. This could become a formalized process, though it raises sensitive issues around jurisdiction and privacy. On the international front, the event bolstered allied cyber cooperation, as seen in the joint advisories. It may serve as a case for advocating norms at forums like the UN, including prohibitions on espionage targeting law enforcement or critical civilian infrastructure. While idealistic, it could lead to narrower agreements in those areas.

The case can also lead to defense and offense policies. On defense, it supports the news U.S. National Cyber Strategy (released 2023) which advocated for more aggressive measures to secure critical infrastructure to hold rogue actors accountable. The call by some legislators/military to allow more offensive operations like “we are going to go into their networks” (Escobedo, 2024) could shape future policy or ROE for CYBERCOM. There is a delicate balance on how to deter such intrusion without escalating conflict. The United States might adopt a policy of more public attribution and sanctions as its chosen deterrent.

In conclusion, the policy impact is likely a tightening of cybersecurity regulations for critical industries, greater momentum for international norms against espionage, and a reinforcement of strategies that blend diplomatic, economic, and possibly cyber offensive tools to deter state-sponsored hacking. Salt Typhoon will be a reference case in policy discussion on why active defense is critical and why purely voluntary approach may fall short. Therefore, Congress should mandate telecom adherence to the same cybersecurity baseline as financial and energy sectors, including reporting timelines, MFA, and firmware logging.

Conclusion

In the current development of cyberwarfare, the 2024 Salt Typhoon espionage efforts against the United States telecommunications carrier is a key example. The operation uncovered advanced persistent flaws in the cyber resilience of vital infrastructure and demonstrated the increasing sophistication and audacity of state sponsored cyber threat actors, particularly from China. This case study provides numerous important lessons by following the campaign from geopolitical motivations to technological operations and finally national level consequences.

Salt Typhoon was unprecedented in scope and consequence. Due to this nine major telecommunications firm were compromised, representing over 60% of United States backbone infrastructure traffic, along with several global peers (Madhani, 2024). The attackers gained persistent access to infrastructures, enabling covert siphoning of metadata, lawful intercept records, and even communication of United States officials and foreign allies (Nakashima, 2024). According to multiple government officials, this ranks as the most severe breach of telecommunications infrastructure in the United States history.

The campaign exemplified elite tradecraft: exploitation of zero-day vulnerabilities, stealthy persistence using “living-off-the-land” methods, and cross-network pivoting through trusted peering relationships. Yet their success was aided by relatively elementary gaps on the defenders’ side due to unpatched network gear and administrator accounts lacking MFA (Madhani, 2024). While APTs bring sophisticated tools, even modest security upgrades (firmware hardening, MFA enforcements) might have exposed or disrupted the intrusion earlier.

The operation had a significant impact even though there were no immediate outages. Large-scale incident response activities, urgent CISA advisories, forced remediation in telecom environments, and modifications to senior U.S. officials' communications procedures were all brought about by it (Madhani, 2024).

This case is also a call to action for stakeholders to strengthen their cybersecurity hygiene and practices. Governments must ensure that important sectors in the country's infrastructure implement a robust security posture and transparent reporting, holding them up to a standard as well. To reach that baseline of resilience, sector-wide measures backed by federal financing and legislation may be required.

References

Nakashima, E. (2024, November 22). Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history.’ *The Washington Post*. https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/

Salt Typhoon | NJCCIC. (n.d.). https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/salt-typhoon

Madhani, A. (2024, December 4). *White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign | AP News*. AP News. https://apnews.com/article/china-hack-us-telecoms-salt-typhoon-88cabc592dae2fa870772c5ce4ace5ea

Lumen Technologies. (2025, October 29). *Taking the crossroads: The Versa director zero-day exploitation*. Lumen Blog. https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation/

Wikipedia contributors. (2025, October 20). *2024 global telecommunications hack*. Wikipedia. https://en.wikipedia.org/wiki/2024_global_telecommunications_hack

Harris, B. (2025, July 21). Salt Typhoon’s deepest breach yet: Why the U.S. military now assumes it’s compromised. *Covert Access Team*. https://covertaccessteam.substack.com/p/salt-typhoons-deepest-breach-yet

Satter, R. (2024, December 4). “Large number” of Americans’ metadata stolen by Chinese hackers, senior official says. *Reuters*. https://www.reuters.com/technology/cybersecurity/large-number-americans-metadata-stolen-by-chinese-hackers-senior-official-says-2024-12-04/

Salminen & Kotfica, *(*2024, December 23*)* Salt Typhoon Cyberattack Prompts Action from FCC, CISA, FBI, and More. https://www.hoganlovells.com/en/publications/salt-typhoon-cyberattack-prompts-action-from-fcc-cisa-fbi-and-more

Escobedo, R. (2024, December 18). *U.S. begins to retaliate against China over hack of telecom networks*. CBS News. https://www.cbsnews.com/news/u-s-retaliates-against-china-hack-telecom-networks/

Page, C. (2025, February 24). Meet the Chinese ‘Typhoon’ hackers preparing for war. *TechCrunch*. https://techcrunch.com/2025/01/10/meet-the-chinese-typhoon-hackers-preparing-for-war/