

Salt Typhoon’s Cyber Espionage: Applying the Diamond Model and Assessing Policy Governance

Mitchell Bardsley
mbardsley3@gatech.edu

Abstract—The People’s Republic of China (PRC)–sponsored advanced persistent threat (APT) known as Salt Typhoon conducted a sustained cyber campaign against United States telecommunications providers from 2023 to 2024, resulting in widespread compromise of critical infrastructure and exposure of sensitive communications metadata and law enforcement systems (Miller et al., 2024). This paper applies the Diamond Model to analyze the intrusion, systematically identifying the adversary, capabilities, infrastructure, and victims, extending the framework through social-political and technological meta-features. Living-off-the-land techniques, exploitation of unpatched Cisco vulnerabilities, and abuse of native network protocols enabled covert, long-term persistence and data exfiltration with minimal detection. Evaluating organizational, national, and transnational policy responses, this paper concludes that enforceable national-level centered upon vulnerability disclosure, supply chain accountability, and coordinated federal oversight are the most effective means to mitigate future nation-state campaigns.

1 INCIDENT OVERVIEW

In 2024, the PRC-sponsored APT known as Salt Typhoon conducted a series of cyber attacks targeting United States telecommunication firms, affecting over 80 U.S. and global firms (Miller et al., 2024). Salt Typhoon exploited Cisco device operating system (OS) vulnerabilities and abused legitimate administration tools in order to conduct lateral movement across networks and domains and obtain network information, sensitive communications data, and metadata (Dimitrov et al., 2025).

Data exfiltrated included customer call records, call and message metadata, IP addresses, phone numbers for over a million users (Barret et al., 2024), private communications traffic involving governmental and political personas, and

information that had been subject to U.S. law enforcement requests issued under judicial authority (Cybersecurity and Infrastructure Security Agency [CISA], 2024). Table 1 outlines key milestones that the threat actors accomplished and subsequent response actions by U.S. parties over the eight-month period of attacks:

Table 1—Salt Typhoon Campaign Timeline (May 2023 – Jan 2024).

Date	Attack Activity Description
May 2023	Begins reconnaissance of telecom endpoints with passive scans; harvest credentials.
June 2023	Exploits multiple Cisco routers with unpatched vulnerabilities.
July 2023	Utilizes routers as lateral movement pivot points to compromise surveillance systems and reuse credentials across domains.
August 2023	Deploys persistent backdoor; encrypted command and control (C2) tunnels built.
September 2023	Begins exfiltration of surveillance metadata, including call data, location data, and unencrypted communications content.
October 2023	Targets Verizon, AT&T, and Lumen telecom providers via infrastructure-level compromise.
November 2023	Government agencies receive breach intelligence, conduct investigations, and propose remediation steps.
January 2024	CISA and the FCC issue public disclosures; U.S. treasury imposes sanctions on cyber entities with assessed PRC affiliation.

Note. Data from Urbanczy, J., Skoumal, C., Elshareif, M., Sultana, H., & Plass, M. R. (2025). State-Sponsored Intrusions and Critical Infrastructure: A Case Study of the Salt Typhoon Cyberattack on U.S. <https://doi.org/10.36227/techrxiv.175085869.97198541/v1>

After the incident became public, multiple U.S. government agencies and services issued coordinated responses, including sanctions, advisories, and mitigation guidance (Urbanczy et al., 2025). The Department of the Treasury sanctioned organizations associated with the Chinese threat actor (United States Department of the Treasury [USDT], 2025) while both the FCC (Federal Communications Commission) (FCC, 2024) and CISA (CISA, 2024) published technical advisories and detailed summaries of the incident.

The multitude of persistent and widely affecting attacks that Salt Typhoon conducted over an extended period represent, in addition to responses, geopolitical and technical complexity. To better understand the underlying

intrusion dynamics, the incident can be analyzed using the Diamond Model. This framework provides a structured method for identifying the relationships between the adversary, their capabilities, infrastructure, and victim entities, while also revealing broader socio-political and technological meta-features.

2 THE DIAMOND MODEL

To best place the Salt Typhoon campaign into context with the Diamond Model, the intrusion can be summarized: The Salt Typhoon APT utilized existing vulnerabilities in Cisco network devices, credential harvesting, and lateral movement techniques to compromise these network devices and exfiltrate call records, network data, and communications metadata from U.S. telecommunications companies. The events depicted in Table 1 provide a foundation for analyzing these sequential actions. Figure 1 depicts analytic pivoting from the adversary feature to the victim feature:

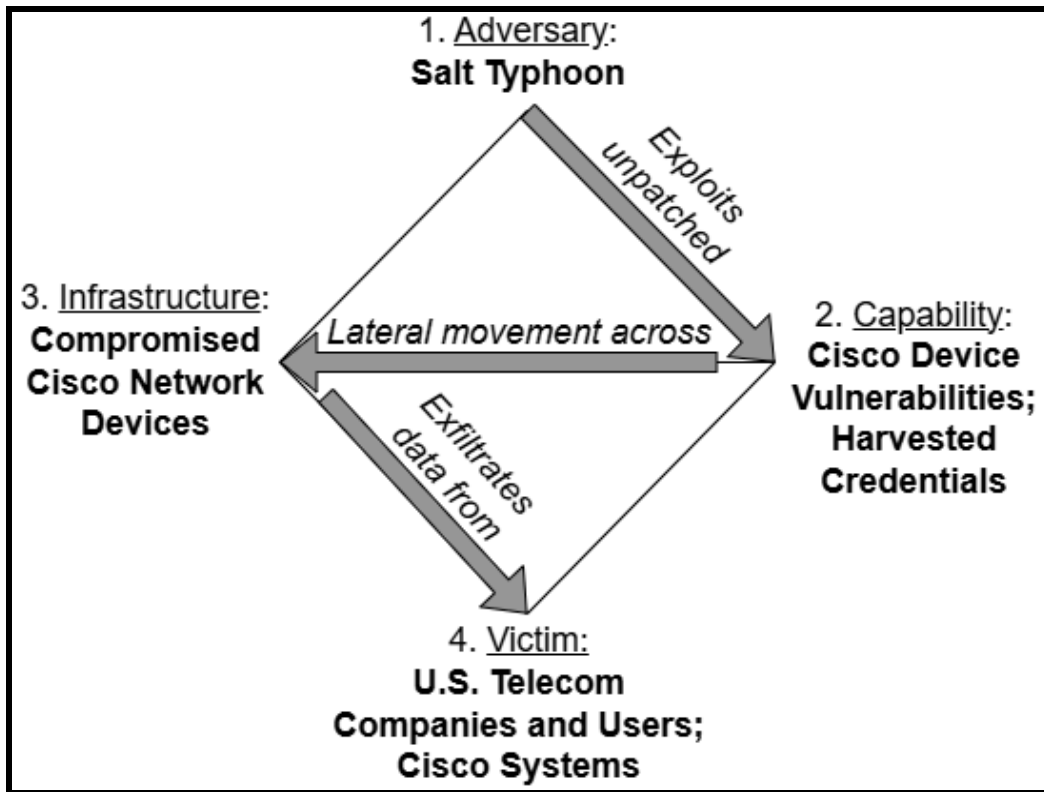


Figure 1—Analytic pivoting of a Diamond Model of the Salt Typhoon campaign. The model summarizes the linear path taken from the attack entity to the victim entities and their information.

Each feature vertex, as well as the interaction edges between each feature vertex, are described in detail in the following sections.

2.1 Adversary

The PRC state-sponsored APT, Salt Typhoon, was the adversary operator in the attack, as the top vertex of the Diamond Model, leveraging capabilities against U.S. infrastructure to victimize personal and government data of Americans. The adversary was attributed to the PRC Ministry of State Security (MSS) as well as three state-owned enterprises: Sichuan Juxinhe Network Technology Co. Ltd., Beijing Huanyu Tianqiong Information Technology Co., Ltd., and Sichuan Zhixin Ruijie Network Technology Co., Ltd. (United States National Security Agency [NSA] et al., 2025). These enterprises are known to have provided network services and products to the PRC's People's Liberation Army (PLA) and intelligence support to the MSS (NSA et al., 2025). They have also been subject of foreign intelligence investigations, of which have discerned the companies' cybersecurity priorities, computer network exploitation activities, and ties to the Chinese Communist Party (CCP) (Insikt Group, 2025), all of which strongly correlate to Salt Typhoon's campaign. Therefore, despite Beijing's public insistence that their government is not responsible for the intrusion (Volz et al., 2024), the PRC's government and its state-sponsored entities can be identified as likely adversary customers.

Salt Typhoon could be quickly attributed to a nation-state due to the large-scale, extensive, and persistent targeting of infrastructure critical to communications. The quality and breadth of persistence, number of vulnerabilities that the group was able to exploit across complex domains, and the cyber attack of companies with international presence and multibillion dollar revenues demonstrated the adversary operator's technical skill and thorough target understanding. Finally, similar telecommunications intrusions were reported in Europe and Asia (Dimitrov et al., 2025), demonstrating the APT's objectives broadening beyond mere hacktivism, terrorism, or extremism, but supporting strategic objectives against Western countries.

Central to investigations and intrusion analysis succeeding the intrusion were the specific capabilities that Salt Typhoon levied, launching attacks with minimal traces but maximum impacts.

2.2 Capability

Salt Typhoon primarily guided capability use, depicted on the right vertex of the Diamond Model, with living-off-the-land techniques against unpatched vulnerabilities of core network components, relying heavily on capability capacity and C2 to maximize the adversary arsenal of exploits. Salt Typhoon's attack methodology centered on exploitation of previously identified vulnerabilities in telecommunications hardware and software, targeting Cisco's IOS XE network operating system and configurations (NSA et al., 2025).

Following successful intrusion, the threat actors established persistence and facilitated lateral movement using admin credentials (Urbanczy et al., 2025) to broaden the attack surface via privilege escalation. By refraining from deploying external malware, Salt Typhoon minimized detection, rendering traditional endpoint detection and response (EDR) mechanisms largely ineffective and allowing for extended persistence (Insikt Group, 2025).

In order to quickly navigate the network environments, Salt Typhoon conducted C2 operations via Generic Routing Encapsulation (GRE) tunnels, virtual private network (VPN) tunnels (Insikt Group, 2025), and a GhostSpider backdoor tool (Urbanczy et al., 2025). GRE is a standard tunneling protocol natively supported on Cisco routing hardware and is often used to build VPNs, bridge heterogeneous network architectures, or transmit multicast and non-IP traffic across IP-based systems (Basu et al., 2025): exploited by Salt Typhoon to maintain persistence and conceal attack-enabling communications from traditional detection methods. Salt Typhoon then leveraged C2 for clandestine data exfiltration, allowing stolen information to be embedded within GRE packets, escaping standard network monitoring (Insikt Group, 2025).

It is through these capabilities that Salt Typhoon could effectively garner a robust, long-term infrastructure for deep and widespread intrusions.

2.3 Infrastructure

Salt Typhoon compromised U.S.-based telecommunications systems to leverage as Type II infrastructure, depicted on the right vertex of the Diamond Model, by obscuring and maintaining persistence for post-exploitation. Intelligence surveys conducted by Recorded Future's Insikt Group (2025) revealed that Salt Typhoon acquired over a thousand Cisco devices as infrastructure for delivering and

controlling capabilities, including seven C2 nodes rooted in Cisco devices from external-to-U.S. internet service providers (ISP): a U.S. affiliate of a U.K. provider and major providers in South Africa, Italy, and Thailand. Salt Typhoon still leveraged the same Cisco devices globally to pivot and redirect to victims in the U.S., with the goal of either acquiring additional attack vectors or establishing C2. In either case, the APT was able to mask traffic and maximize access to network information, configurations, and ultimately, victim data.

As of November 2025, there are still no publicly disclosed reports that have identified Type I infrastructure such as C2 nodes, devices, or domains to have been fully controlled and managed by Salt Typhoon.

As all infrastructure leveraged by the APT during the telecommunications espionage belonged to the U.S., the specific victims affected by the campaign, both directly and indirectly, become clear.

2.4 Victim

These capabilities were launched by Salt Typhoon across the Cisco device infrastructure against victim providers in the U.S., depicted on the bottom vertex of the Diamond Model, and includes Verizon, AT&T, T-Mobile, Lumen (Urbanczy et al., 2025), and ISPs in other countries (Insikt Group, 2025). Victim personas included high ranking government officials, politicians, presidential campaign affiliates (Barret et al., 2024), provider customers, and their call records and metadata (CISA, 2024). Included in victim assets was lawful wiretapping network infrastructure (Krouse et. al, 2024).

Vulnerabilities as sub-features and susceptibilities are the technical victims that were the key campaign enablers. The most critical of these were CVE-2023-20198 and CVE-2023-20273, which enable unauthorized actors to execute arbitrary commands with elevated administrative privileges (Cisco, 2023), depicted in the campaign's larger context in Figure 2:

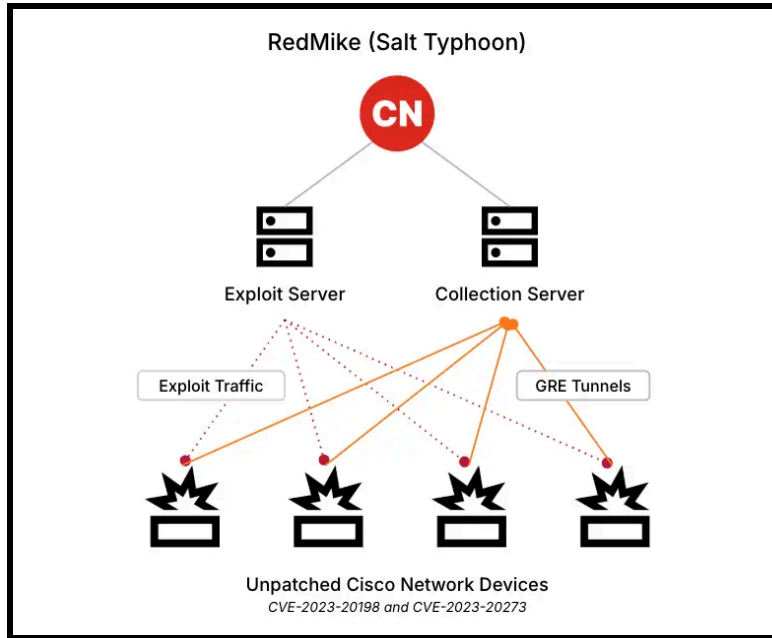


Figure 2—CVE-2023-20198 and CVE-2023-20273 depicted within the context of the intrusion and Salt Typhoon’s exploitation of the Cisco devices. Source: [Insikt Group, 2025](#).

Additional susceptibilities exploited included web management plugin command injection and secure firewall management arbitrary file creation vulnerabilities (NSA et al., 2025). Identifying these is the first step toward mitigation, and it is clear from the span of victim personas and assets that Salt Typhoon launched a highly successful campaign.

2.5 Meta-Features

Meta-features will highlight the particularities with Salt Typhoon as a persistent nation-state adversary of the United States. Further, a technology centered approach will underscore the services and protocols that enabled the attack between exploits and the Cisco devices as infrastructure.

2.5.1 Social-Political Meta-Feature

As a nation-state adversary, Salt Typhoon’s actions garnered major geopolitical implications. The PRC considers cyber warfare to be an integral component of the country’s strategic pre-positioning for maintaining a longer term information advantage, particularly against the U.S. (Dimitrov et al., 2025). Figure 3 depicts this relationship within the context of the Diamond Model:

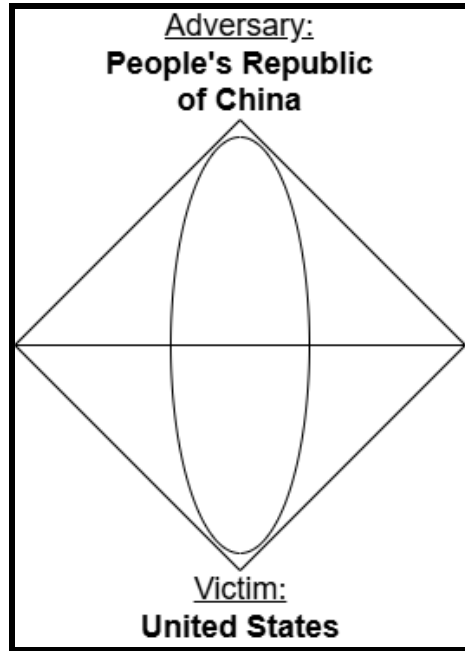


Figure 3—Social-Political Meta-Feature for the Diamond Model of Salt Typhoon’s campaign, depicting national implications not typically depicted by a basic Diamond Model.

National security for the PRC is spearheaded by cyber espionage against critical infrastructure. Exfiltrating valuable administrator credentials, intellectual property, and actionable intelligence (Dimitrov et al., 2025) are critical U.S. products for the PRC’s consumption. These force national actions by the U.S. to significantly strengthen cybersecurity posture to counter living-off-the-land techniques, especially in anticipation of stronger and more lucrative attacks.

Evaluated by the extreme strength in budget and technology, imposed costs of trillions of dollars on a victim of interest, and an enduring rivalry over markets and global influence, it is clear that the motivation for more Salt Typhoons and large-scale cyber attacks is historic and will only increase.

2.5.2 Technology Meta-Feature

Salt Typhoon primarily targeted device management services, repurposed legitimate network management and diagnostic utilities such as Simple Network Management Protocol (SNMP), Telnet, and Secure Shell (SSH) (Insikt Group, 2025). Web Services Management Agent (WSMA) endpoints and Secure File Transfer Protocol (SFTP), Remote Desktop Protocol (RDP), and File Transfer Protocol (FTP) were used as capabilities for obfuscating data exfiltration (NSA et

al., 2025). For infrastructure, virtual private servers (VPSs) and compromised intermediate routers were, without bias towards ownership, leveraged by Salt Typhoon (NSA et. al, 2025). This relationship is shown with the Diamond Model in Figure 4:

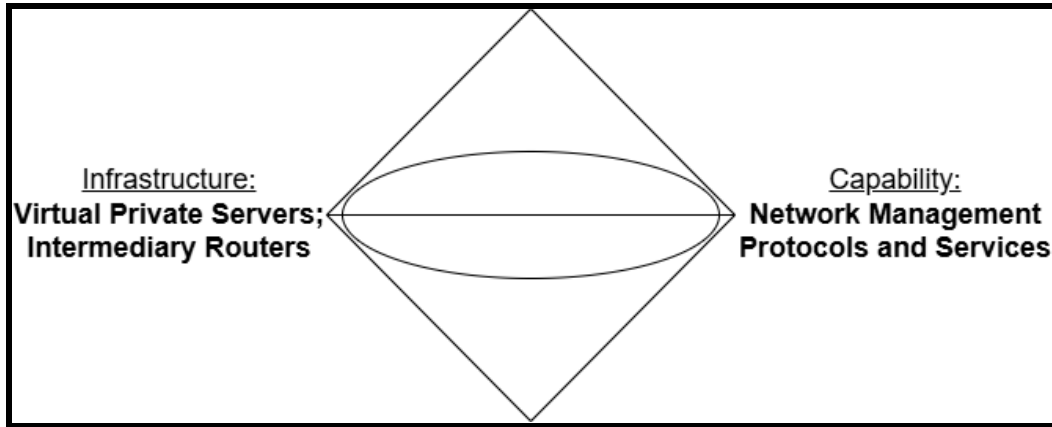


Figure 4—Technology Meta-Feature for the Diamond Model of Salt Typhoon's campaign, depicting specific additional malicious activities not typically analyzed by a basic Diamond Model.

Combining seemingly harmless management and monitoring tools with non-specific and vulnerable network devices allowed for an extremely covert campaign by Salt Typhoon. This highlights the importance of intense and updated cybersecurity policy scrutiny and increased attention towards defensive cyber postures across all governance layers.

3 POLICY ASSESSMENT

Each level of policy for this intrusion is addressed in accordance with historic progress, the frequency of related attacks, and associated risks. A recommendation for the most effective policy level is also provided.

3.1 Organizational Policy

At the organizational level, a large part of the intrusion was in the market category: Cisco failed to address vulnerabilities in their produced devices. In 2023, Cisco did issue free software updates, fixed releases, and recommended to disable the HTTP server feature upon recognition of the vulnerabilities, but this was clearly not enough to prevent the intrusion.

As for the cooperative networks: the victim telecommunications providers did not immediately comment on the attack (Volz et al., 2024), but Reuters reported in December of 2024 that AT&T and Verizon contained the intrusion and eliminated the threat from their networks.

As nation-state attacks become more common, it will certainly be necessary for companies to update policies, but considering the scale of these enterprises extends beyond mere company policies and occurs at strategic levels, and many of these vulnerabilities can and will extend beyond proprietary devices, there is a risk of massive blind spots that will never be addressed.

3.2 National Policy

At the national level, government entities in the hierarchy immediately sought investigations and policy changes, indicative of the level of change required to address the issue. The FCC proposed the issuance of a declaration to affirm telecommunications carrier network security requirements (FCC, 2024), the U.S. Treasury levied sanctions (USDT, 2024), CISA and the FBI issued a joint statement (CISA, 2024), and the U.S. Congress called for investigations and affirmed the roles of established executive cyber entities (Jaikaran, 2025). While inspired by the Salt Typhoon attacks, the assessed frequency and impact of associated APT attacks within the past decade, to include the months of persistent attacks from Volt Typhoon and Flax Typhoon (Jaikaran, 2025), also played a factor. While highly reactive in nature, these responses set the foundation for proactive actions.

The significant geopolitical risk with national action, however, is escalating tensions and inviting more covert espionage, specifically against the U.S. Domestically, companies may try to subvert requirements for the sake of profits, and it is impossible to estimate to what extent companies may subvert them, nor how efficiently they will be held accountable. Nonetheless, these risks may need to be acceptable to prevent future breaches.

3.3 Transnational Policy

At the transnational level, while there is an international advisory and some regulatory action, there is not yet a fully binding international legal framework that specifically addresses Salt Typhoon or similar campaigns with clear enforcement or consequence mechanisms, nor is there any indication that such a

proactive policy, treaty, or agreement with adversary-enabling nation-states would prevent future large-scale attacks.

Transgovernmental organizations such as the ISA Global Cyber Alliance recognized that cyber attacks against critical infrastructure increased by 30% in 2023 (Amos, 2024) and provided cybersecurity defense recommendations. However, acknowledging hierarchies, no sanctioning or enforcement occurs at the international level. This is a significant risk that will persist as nation-state breaches become more common.

4 RECOMMENDATION

Public policy changes at the national level must be the top priority for governance to most effectively combat future nation-state APT attacks against critical national infrastructure that underpins cross-sector communications. Vulnerability disclosure mandates, supply chain accountability procedures, and proactive government department and agency coordination, to include the FCC, CISA, and USDT, are the most crucial areas where legal and regulatory change is necessary to prevent devastating espionage campaigns, of which outweigh the comparatively smaller risk associated with harming national relations. Additionally, as concluded by Urbanczy et al. (2025), automated patch processes, strict access control measures, threat intelligence sharing and actioning, and intentional resilience and hardening mandates must be implemented in technical policy at the national level to be best enforced.

5 REFERENCES

1. Amos, Z. (2024). Defending against state-sponsored cyberattacks in 2025. *Defending Against State-Sponsored Cyberattacks in 2025*. <https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025>
2. Barrett, D., Swan, J., & Haberman, M. (2024, October 25). Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance. *The New York Times*. <https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html>
3. Basu, A., & Zhang, W. (2025, April 18). Understand GRE Tunnel Keepalives. *Cisco.com*. <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118370-technote-gre-00.html>

4. Cisco. (2023, October 16). Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature. Cisco.com. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>
5. Cybersecurity and Infrastructure Security Agency. (2024, November 13). Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure. CISA. <https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications>
6. Dimitrov, D., & Andreev, E. (2025). China's strategic competition in cyberspace. volt typhoon and salt typhoon as a projection of power, a more aggressive posture and a future beyond espionage. ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2, 115–122. <https://doi.org/10.17770/etr2025vol2.8618>
7. Federal Communications Commission. (2024, December 5). FACT SHEET: IMPLICATIONS OF SALT TYPHOON ATTACK AND FCC RESPONSE. FCC.gov. <https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf>
8. Insikt Group. (2025, February 13). RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers. Recorded Future. <https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices>
9. Jaikaran, C. (2025, January 23). Salt Typhoon Hacks of telecommunications companies and federal response implications | congress.gov | library of Congress. Congress.gov. <https://www.congress.gov/crs-product/IF12798>
10. Krouse, S., Volz, D., Viswanatha, A., & McMillan, R. (2024, October 5). U.S. Wiretap Systems Targeted in China-Linked Hack. The Wall Street Journal. <https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>
11. Miller, M., Bazail-Eimil, E., & Gramer, R. (2024, December 12). We need to talk about Salt Typhoon. Politico. <https://www.politico.com/newsletters/national-security-daily/2024/12/12/we-need-to-talk-about-salt-typhoon-00183727>

12. Misra, S., & Shepardson, D. (2024, December 29). AT&T, Verizon targeted by Salt Typhoon cyberespionage operation, but networks secure. Reuters. <https://www.reuters.com/technology/cybersecurity/chinese-salt-typhoon-cyberespionage-targets-att-networks-secure-carrier-says-2024-12-29/>
13. United States Department of the Treasury. (2025, January 17). Treasury sanctions company associated with salt typhoon and hacker associated with Treasury compromise. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy2792>
14. United States National Security Agency (NSA), United States Cybersecurity and Infrastructure Security Agency (CISA), United States Federal Bureau of Investigation (FBI), United States Department of Defense Cyber Crime Center (DC3), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian Centre for Cyber Security (Cyber Centre), Canadian Security Intelligence Service (CSIS), New Zealand National Cyber Security Centre (NCSC-NZ), United Kingdom National Cyber Security Centre (NCSC-UK), Czech Republic National Cyber and Information Security Agency (NÚKIB), Finnish Security and Intelligence Service (SUPO), Germany Federal Intelligence Service (BND), Germany Federal Office for the Protection of the Constitution (BfV), Germany Federal Office for Information Security (BSI), Italian External Intelligence and Security Agency (AISE), Italian Internal Intelligence and Security Agency (AISI), Japan National Cybersecurity Office (NCO), Japan National Police Agency (NPA), Netherlands Defence Intelligence and Security Service (MIVD), ... Spain National Intelligence Centre (CNI). (2025, September 3). Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System. CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a>
15. Urbanczy, J., Skoumal, C., Elshareif, M., Sultana, H., & Plass, M. R. (2025). State-Sponsored Intrusions and Critical Infrastructure: A Case Study of the Salt Typhoon Cyberattack on U.S. <https://doi.org/10.36227/techrxiv.175085869.97198541/v1>
16. Volz, D., & FitzGerald, D. (2024, October 11). U.S. Officials Race to Understand Severity of China's Salt Typhoon Hacks. The Wall Street Journal. https://www.wsj.com/politics/national-security/u-s-officials-race-to-understand-severity-of-chinas-salt-typhoon-hacks-6e7c3951?gaa_at=eafs&gaa_n

=AWEtsqfagAjw0Fm0TU9ASzesosu9BtWOSPgR1A7HQ_BfsGidY3Z4m9
Q3K4X11UbXY2s%3D&gaa_ts=690eb1e6&gaa_sig=hj9Y8h1JWAw20fbJ-Bk
kesqhvwjZ6xpfXM__uccoMVuXKG4QqOGGR_xWwNHLnvVcaflihHQf5
3oXbOF5PP3nlw%3D%3D