Salt Typhoon: Strategic Cyber-Espionage and the Weaponization of U.S. Telecommunications Infrastructure — A Case Study and Technical Analysis

Ankita Varma, Jamie Crosby, Ekema-Ndoh Ebone

Department of Information Technology and Management, Illinois Institute of Technology

September 7, 2025

Abstract

The 2024 Salt Typhoon cyberattack represents one of the most extensive and strategically significant cyber-espionage campaigns in recent history. Orchestrated by a Chinese state-sponsored group, the attack targeted U.S. telecommunications infrastructure, compromising major providers and exfiltrating sensitive data from over one million Americans, including high-level political figures. This paper examines the technical methods used, such as SS7 exploitation, CVE-based intrusions, and custom malware deployment, as well as the broader geopolitical motives behind the operation. It explores the cascading impact across critical sectors including defense, healthcare, and intelligence, and evaluates the international and national responses, including sanctions, legal actions, and cybersecurity reforms. The findings reveal a deeply concerning vulnerability in global digital infrastructure and underscore the urgent need for decisive, coordinated action. Without robust cybersecurity policies, improved threat attribution, and strengthened international cooperation, the long-term consequences of such attacks may continue to undermine democratic institutions and national security.

Keywords: cyber-espionage, telecommunications breach, cybersecurity policy, Salt Typhoon, critical infrastructure, JumbledPath

Salt Typhoon: Strategic Cyber-Espionage and the Weaponization of U.S. Telecommunications Infrastructure — A Case Study and Technical Analysis

As global reliance on digital infrastructure increases, the world's cybersecurity is under unprecedented strain. Modern attacks continue to increase in scale, sophistication, and strategic intent. For example, the Salt Typhoon cyber-espionage group, based in China, emerged as a significant threat during its past activities, having penetrated the U.S. critical infrastructure. They began infiltrating telecom networks to steal voter information, intercept communications, interfere with election security, and collect sensitive data. The move intensified the use of cyberattacks as policy tools in a rapidly changing geopolitical landscape, as well as tactics employed in ongoing assaults. The primary concern remains the specific target of why the People's Republic of China (PRC) - sponsored hackers have been infiltrating U.S. telecommunications firms. Therefore, the paper examines Salt Typhoon's Chinese-backed cyber-attacks on telecom systems, revealing the geopolitical weaponization of cyberspace to influence elections and compromise democratic resilience.

Salt Typhoon executed a coordinated cyber-espionage campaign against telecom infrastructure during elections to gain persistent access and gather intelligence. Some of the cybersecurity products, such as firewalls used to protect large organizations, were found to have technical vulnerabilities that Salt Typhoon exploited (Forno, 2024). The attackers penetrated the network using more traditional tools and expertise to spread their influence, collect additional information, remain undetected, and install malware for later use. The article further states that the FBI Council believes Salt Typhoon gave Chinese authorities access to vast quantities of records detailing where, when, and with whom individual persons were communicating. In others, they said that Salt Typhoon also provided access to the contents of text messages and phone calls. The attackers installed malware and backdoors that enabled them to intercept communications, spy on political leaders, and gather data related to voters. Therefore, Salt Typhoon's case demonstrates the fragility of telecom systems in safeguarding electoral integrity.

Primary Motives for the Attack

China's state sponsorship of Salt Typhoon reflects motives of political influence, counterintelligence, and strategic dominance. Intelligence testing showed that China is involved in cyber operations to spy on elections, manipulate political results, and gather personal and government-sensitive information. Forno (2024) recommends that the Chinese government employ strategies aimed at influencing legislators and the public in favor of more beneficial policies towards China. Meanwhile, the Chinese government is aspiring to be the greatest superpower in the world by engaging in predatory lending and business conduct, systematically stealing intellectual property, and engaging in audacious cyber-attacks. China's work is aimed at businesses, academic institutions, researchers, lawmakers, and ordinary people, and will need a whole-of-society response.

As the world’s digital landscape continues to grow, the threats that we face as a nation grow in tandem. Recently, our nation has witnessed what is now being called the largest cyber warfare attack that we have ever identified. Though this attack's true intent has yet to be defined, counterintelligence and cyber espionage are at play. “The Oxford Bibliographies definition of cyber espionage states that cyber espionage is the exploitation of cyberspace for the purpose of accessing and collecting confidential data" (Godefrey, 2022).

Timeline of the Tactics, Techniques and Procedures

While it is known that Salt Typhoon began infiltrating the US telecom systems as early as 2019, it is believed that in January 2024 Salt Typhoon began conducting thorough reconnaissance throughout the United States telecom systems. Multiple telecom companies were compromised and include, but are not limited to, Verizon, T-Mobile, and AT&T. Salt Typhoon is a state sponsored group organized by China's Ministry of Security (MSS) and People's Liberation Army (NSA, 2025). It was discovered that they were performing signaling system 7 attacks and compromised numerous networking devices. The signaling system 7 attacks use the SS7 protocol, developed in the 1970's and connects major network communications worldwide. This protocol allows access to the same type of surveillance mechanisms used by US governmental intelligence agencies. This technology is utilized by digital signaling networks which enable wireless communications. Since SS7's creation, it has been used heavily in services like short message service (SMS). Attackers use SS7 to exploit and intercept voice and text message communications which utilize mobile phone communications instead of Wi-Fi communications (Weinberg, 2023).

Common Vulnerabilities and Exposures

By March of 2024 there were coordinated attacks on the United States telecom companies and their infrastructure. They exploited internal routers and used them to gain further access to additional networks. This access enabled them to modify configurations and edit routing tables. They accessed these networks by exploiting multiple CVEs found in Cisco, Palo Alto, and Ivanti products. Once they gained access, they were able to maintain persistent control by modifying Access Control Lists (ACLs), opening previously closed ports, creating tunnels, manipulating configurations, creating new accounts, updating routing tables, deleting logs, and exfiltrating sensitive data. During the attack, Salt Typhoon utilized multiple known CVEs on networking communication devices. These CVEs were monumental in successfully completing the actions that they took to further enumerate throughout the connected networks. Cisco devices that have smart install technology in their Cisco IOS software allowed attackers to infiltrate through a data packet vulnerability, also known as CVE-2018-0171 (CVSS Score 9.8). The attackers sent a Smart Install message to the device on TCP port 4786 to cause a buffer overflow. A buffer overflow is a common tactic that attackers use to overload a system's temporary storage. By forcing too much data onto a buffer, or writing outside of the limitations of memory allocated, attackers can corrupt data, crash the program, or execute malicious code (OWASP, 2025). Cisco's software vulnerability allowed attackers to remotely authenticate in and start reloading the device. Furthermore, they could perform a Denial-of-Service, cause an indefinite loop, or execute arbitrary code (Cisco, 2025). Investigators speculate that the group was also able to obtain access through compromised credentials, though the origination of the credentials is not yet fully known (Lakshmanan, 2025). An additional CVE that was used in this attack was CVE-2024-21887 (CVSS 9.8), a command injection vulnerability found in web components of Ivanti Connect Secure and Ivanti Policy Secure on Ivanti's devices. This vulnerability allows attackers to authenticate in and perform arbitrary commands on the device. Another critical CVE, CVE-

2024-3400 (CVSS 10), was also used in the attack. This critical vulnerability is found on Palo Alto devices and allows for command injections through arbitrary file creation. The GlobalProtect feature found on Palo Alto devices enables attacks to perform arbitrary code execution with high level root privileges on these firewalls. By exploiting these CVEs, attackers obtained a tremendous amount of unauthorized access and collected data to perform more reconnaissance. Additional Tactics, Techniques, and Procedures that were used in this attack are as follows: Account Manipulation using SSH authorized keys, brute force password cracking, creating Linux users on compromised network devices through the /etc/passwd and /etc/shadow files, dumping network device configurations to acquire credentials, developed custom malware, exfiltrated data over FTP and TFTP, mapping internal network topology, modify system access control lists and loopback interface addresses on devices, cleared system logs, captured packet data through different network devices, changed device configurations and created Generic Routing Encapsulation tunnels (Mitre, 2025).

Malware Deployment

In June of 2024 custom malware was deployed that had been undetected by implemented detection systems. A Go based malware called JumbledPath enabled the group to monitor network traffic. This malware gave them the ability to capture packets on Cisco devices remotely. According to Cisco Talos, JumbledPath utilized a jump-host and was able to clear logs along the path. Throughout these connections the group was successful in remaining undetected by compressing encrypted data captures and using different connections and jumps. This allowed them to move throughout the networks in ways that they would not have been able to reach on non-public routable devices. Since the malware was compiled as an Executable and Linkable Format (ELF) binary, it was used on the Linux based Cisco networking devices (Cisco Talos, 2025). The JumbledPath malware made it exceedingly difficult to trace the attackers because it was able to hide the data by scrambling it through multiple jump-hosts. Salt Typhoon was very covert in their operation by using jump hosts and “living off the land” by using common commands to fly under the radar and remain undetected.

Scope and Infrastructure Impact

The widespread telecommunications attack on U.S. networks prompted Brett Leatherman, Assistant Director of the FBI’s Cyber Division, to describe it as “one of the more consequential cyber espionage breaches we have seen here in the United States” (Viswanatha & Krouse, 2025). The attack affected over 600 organizations across more than 80 countries, including more than 200 U.S.-based entities spanning sectors such as telecommunications, defense, hospitality, government, and transportation (Anthoney, 2025).

Investigation findings indicate that the United States was the primary target, experiencing the highest level of penetration and compromise. The attackers exfiltrated sensitive data including call and text records of over one million Americans, classified wiretap court filings, U.S. Army National Guard network configuration files, system architecture diagrams, and administrator credentials. Dr. Susan Landau, professor of Cybersecurity and Policy at Tufts University, warns “that cyber-attacks bring the front lines of conflict directly to American citizens[, u]nlike traditional warfare" (Sain, 2025). The impacts of this attack continue to reverberate and may lay the groundwork for more invasive operations in the future.

U.S. Telecommunications Breach and Cross-Sector Impacts

The long-term nature of the breach further underscores its severity. Investigations reveal that Salt Typhoon infiltrated U.S. telecommunications networks as early as 2019 and has persistently gathered data since then (Kapko, 2025; Viswanatha & Krouse, 2025). According to Senator Mark Warner, a member of the Senate Intelligence Committee, attackers were able to listen in on telephone conversations and access unencrypted communications while embedded in the network (Goldman, 2025).

Although major telecommunications companies have taken steps to remove the attackers from their systems, many compromised devices remain unpatched and lack sufficient security measures. Investigations into the full extent of the breach are ongoing, and until all vulnerabilities are addressed, the complete impact of the attack cannot be fully measured.

U.S. Defense Sector Compromise

Beyond the telecommunications sector, Salt Typhoon moved laterally into other areas of U.S. infrastructure, including military networks. Investigations revealed that attackers infiltrated the U.S. Army National Guard's systems, stealing network configurations, system diagrams, administrator credentials, and configuration files. The U.S. Army National Guard operates at both federal and state levels, and in some states, it serves as the exclusive provider of network defense. Its systems contain sensitive information, including the cybersecurity posture of individual states, U.S. Army infrastructure, and personally identifiable information (PII) of cybersecurity personnel. By exfiltrating this data, attackers now possess the intelligence needed to conduct highly targeted, stealth operations and potentially surveil security personnel without detection (Ribeiro, 2025).

Multi-Sector Spread in U.S. Infrastructure

The telecommunications breach served as a gateway to a broader, multi-sector compromise. In addition to disrupting communications infrastructure, Salt Typhoon's attack extended into industries such as transportation, lodging, and military operations, all of which were affected through the theft of telecommunications data. To date, over 80 countries have reported breaches within their systems, and preliminary investigations suggest that individuals in the Washington, D.C. area were specifically targeted (Associated Press, 2024).

US Intelligence Agencies and Data Security

The breach's implications for U.S. national intelligence are among the most alarming outcomes of the Salt Typhoon campaign. While the attack affected multiple sectors, the compromise of intelligence-related data marks a serious escalation in its strategic impact, with far-reaching geopolitical, security, and counterintelligence consequences.

Attackers obtained enough information to triangulate the locations, phone numbers, contacts, and behavioral patterns of individuals involved in national security operations. This includes access to sensitive communications and metadata that could reveal who the U.S. government suspects of espionage, as well as the methods used to monitor them. With this level of insight, adversaries could potentially track intelligence personnel in real time, intercept classified exchanges, impersonate officials, and exploit operational routines to disrupt missions or evade surveillance. The Federal Bureau of Investigation (FBI) is expressing heightened concern that its informants may be endangered due to the potential analysis of call patterns and the theft of call records. These records include phone numbers, source and destination IP addresses, and location data (Sanger et al., 2024).

The stolen data also comprises classified court filings related to wiretap requests submitted by intelligence agencies such as the FBI, National Security Agency (NSA), and Central Intelligence Agency (CIA) (Rissman, 2025; Sain, 2025; Viswanatha & Krouse, 2025). These filings are governed by the Foreign Intelligence Surveillance Act (FISA) of 1978, which authorizes classified surveillance and intelligence collection on foreign powers and agents of interest through requests submitted to the Foreign Intelligence Surveillance Court (FISC) (Bureau of Justice Assistance, 2020; US Foreign Intelligence Surveillance Court, 2025).

The filings detail who is to be surveilled, the rationale behind the surveillance, and the methods to be employed. Once authorized, intelligence agencies conduct sensitive investigations and counterintelligence operations. The theft of these classified court records places critical information about known or suspected spies and informants into the hands of malicious actors. The breach exposed intelligence on suspected spies from several countries, including Russia, Israel, and China, prompting serious concerns about the broader implications for global security and diplomatic relations. Also compromised was "a nearly complete list of phone numbers [that] the Justice Department monitors in its "lawful intercept" system" (Sanger et al., 2024). The attackers obtained unencrypted wiretap request logs containing information related to national security and active intelligence investigations, significantly compromising law enforcement's ability to conduct secure surveillance and track criminal activities (Freeman, 2024).

Security Risks in the 2024 Election

Over the course of a yearslong cyberattack that is estimated to have begun in 2019 and was discovered in 2024, the call records and text messages of more than one million Americans were stolen. Among those affected were President Trump, Vice President Vance, and former Vice President Harris, whose communications were compromised while they were active on the campaign trail. At the time, Vice President Vance was serving as a sitting senator, and former Vice President Harris was still in office. The exposure of their communications presents a serious national security risk.

This breach of telecommunications infrastructure occurred during a critical election period and was part of a broader pattern of international cyberattacks and disinformation campaigns intended to undermine public trust in the United States electoral system and influence voter behavior.

US Surveillance

The attackers intercepted and accessed unencrypted phone calls and text messages in a widespread effort to track and monitor Americans both domestically and abroad. The stolen call records included location data, which enabled the tracking of individuals' movements through their mobile devices (Viswanatha & Krouse, 2025). The volume and detail of the compromised data provided enough information to reconstruct communication networks and physical movements, resulting in a serious invasion of privacy and a decline in public trust.

The Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994, required telecommunications companies in the United States to build lawful access mechanisms that would allow law enforcement agencies to conduct surveillance when authorized. However, this legal backdoor was exploited by Salt Typhoon and continues to be vulnerable.

Continuing Fallout and Lingering Effects

By August 2025, Verizon confirmed that it had "contained" the breach, while a T-Mobile spokeswoman said in a statement "it detected attempts to infiltrate its systems by bad actors. Its defenses "worked as designed to prevent any access to or exfiltration of customer or sensitive information"" (Viswanatha & Krouse, 2025). One of the vulnerabilities exploited was hardware-related and cannot be resolved through a software patch. In response, the United States Government Accountability Office (GAO) has proposed a study to assess the costs of replacing China-made infrastructure and to investigate security vulnerabilities across the country (DiMolfetta, 2025). A comprehensive understanding of the full impact of the attack will remain incomplete until the vulnerabilities are fully addressed and mitigation efforts are completed.

Response

In the aftermath of the Salt Typhoon telecommunications breach, governments and institutions around the world initiated a range of responses aimed at mitigating its impact and preventing future incidents. These included international diplomatic actions, economic sanctions targeting entities linked to the attack, and a series of cybersecurity measures led by the United States government.

International response

Due to the international impact of the Salt Typhoon attack, which affected systems in over 80 countries, 13 nations collaborated to publish a joint cybersecurity advisory. This publication emphasized the scale of the attack's blast radius and demonstrated solidarity in supporting countries that may lack the resources to investigate or defend against such threats. The advisory included detailed guidance on threat hunting, indicators of compromise, and mitigation strategies specific to the Salt Typhoon incident (USA et al., 2025). This unprecedented level of international coordination increases diplomatic pressure on China, signals a shared understanding that the attacks are connected, and advocates for the adoption of global cybersecurity standards. The mass publication also serves as a deterrent to future attackers.

In April 2025, *The Wall Street Journal* reported a secret meeting of Chinese officials, suggesting a link between the cyber-attacks and increased U.S. support for Taiwan. Although the statement was indirect and veiled, its underlying threat was clear. Since then, U.S.–China relations have remained tense, locked in an ongoing trade war (Volz, 2025).

U.S. Sanctions and Legal Measures

Complementing the broader international response, the United States implemented targeted diplomatic and legal actions. The U.S. Treasury Department identified three Chinese cybersecurity companies linked to the attack and imposed economic sanctions on one company and one individual hacker. In parallel, the U.S. Department of Justice indicted more than 12 Chinese nationals in connection with the breach (Schappert, 2025). However, these measures have had limited impact. Salt Typhoon re-attacked telecommunications infrastructure between December 2024 and January 2025, employing similar mechanisms and tactics (Kapko, 2025).

U.S. Governmental Cybersecurity Response

Considering Salt Typhoon’s persistent threat and the limited impact of initial sanctions, the U.S. federal government has escalated its response through a series of coordinated actions aimed at strengthening national cybersecurity and deterring future attacks. On December 5, 2024, the Federal Communications Commission (FCC) published a fact sheet acknowledging the impact of the infiltration into national telecommunications systems, which affected over nine major providers. The document also highlighted the cascading effects on other critical infrastructure sectors, including healthcare. In response, the FCC mandated annual cybersecurity certifications and clarified that the Communications Assistance for Law Enforcement Act (CALEA) applies to both equipment and network management used by telecommunications carriers (FCC, 2024). The scope and severity of the attack were so extensive that the Federal Bureau of Investigation (FBI) reversed its longstanding opposition to encrypted communications and endorsed joint guidance recommending their use (Sain, 2025). One intelligence official described the incident as a “weaponization of our communications infrastructure” (Sayegh, 2025).

Tracing Salt Typhoon's activities directly to China posed significant challenges due to the sophisticated obfuscation techniques employed by the group. Malware signatures were similar to other APTs (Advanced Persistent Threats), so the investigators were wary when attributing the attacks. In this way, they could crack the PINs, or backdoors, that telephone companies offer law enforcement to seek court-authorized surveillance of phone numbers during investigations. It remains the same portal that U.S intelligence uses to spy on foreign targets within the United States. Prasad et al. (2025) indicates that attackers are increasingly using autonomously adapting malware, intelligent botnets, and algorithmically optimized phishing campaigns. Its variants, trained on large language models (LLMs), bear the telltale linguistic structures in their code that are deliberately designed to be misinterpreted by attribution engines, producing completely novel obfuscation vectors. Attribution difficulties embolden attackers, as uncertainty complicates retaliation and collective defense measures.

International Response

Fortunately, the global response included condemnation, sanctions, and cybersecurity reinforcements; however, its effectiveness was limited. The U.S. and Britain also sanctioned high-level Chinese hacking units. They have charged the top spy agency in Beijing with a years-long attempt to install malware in American electrical grids, defense systems, and other critical infrastructure and steal the voting rolls of 40 million British citizens (Sanger & Landler, 2024). Multilateral collaboration served to increase awareness and fortify defenses, but the absence of an international binding cyber law diminished deterrence. Salt Typhoon underscores the need for developing more robust, multi-jurisdictional strategies in response to state-sponsored cyber aggression.

Solution to the Attack

Consequently, organizations need to look beyond the news to gather information about this attack, as well as to various free, commercial, or ad hoc threat intelligence feeds and informal professional communities, to stay current on attacker tactics and techniques—and how to counter them. The ongoing inquiry by the U.S. government into the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure has uncovered a vast and extensive cyber espionage activity (FBI National Press Office, 2024). They still provide technical support, quickly disseminate information to help other potential victims, and strive to enhance cyber defenses in the commercial communications industry. Businesses and governments are also advised to properly staff and fund their information technology departments and cybersecurity initiatives to address their specific requirements, ensuring that best practices and legal policies are enforced (University of Maryland, 2024). The threat of groups such as Salt Typhoon can only be minimized through regular check-ups on technological innovation, the law, and joint actions.

Conclusion

In conclusion, Salt Typhoon refers to the surge in cyber activity by states aimed at disrupting elections, counterintelligence, and cyber espionage. The attack exposed potential vulnerabilities in the core telecom systems that underpin electoral integrity and stealing sensitive data. Active measures in cyber defense and international coordination play a critical role in reducing such threats. By having the ability to listen to conversations, adversaries can follow top secret conversations that may detail intelligence reports, military plans, and secret information about topics that foreign national leaders may have otherwise never known about. This not only allows adversaries to have the upper hand in negotiations but can also aid them with the destruction of critical infrastructure during the time of a national emergency, particularly if they are able to misconfigure communications systems to the point of full inoperability. The response to these threats should include robust defense policies, international cooperation, and measures to enhance nations' resilience to cyber espionage. Protecting democracy in the digital world means strength, vigilance, and concerted international efforts against nationally sponsored cyber war. The depth of this attack illustrates how important telecommunications systems are to other nations’ governments.

References

Anthoney, C. (2025, September 5). *China-Linked Salt Typhoon hackers target global telecom and critical sectors*. https://www.paubox.com/blog/china-linked-salt-typhoon-hackers-target-global-telecom-and-critical-sectors

Associated Press. (2024, December 27). *Massive Chinese espionage scheme hit 9th telecom firm, US says*. Voice of America. https://www.voanews.com/a/massive-chinese-espionage-scheme-hit-9th-telecom-firm-us-says/7916311.html

Bureau of Justice Assistance. (2020, October 1). *The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance*. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

Cisco Talos. “Weathering the Storm: In the Midst of a Typhoon.” *Cisco Talos Blog*, 20 Feb. 2025, blog.talosintelligence.com/salt-typhoon-analysis/.

DiMolfetta, D. (2025, January 6). *GAO mulls cost evaluation of nationwide telecom hardware replacement*. Nextgov.Com. https://www.nextgov.com/cybersecurity/2025/01/gao-mulls-cost-evaluation-nationwide-telecom-hardware-replacement/401963/

FBI National Press Office. (2024). Joint Statement from FBI and CISA on the People’s Republic of China Targeting of Commercial Telecommunications Infrastructure | Federal Bureau of Investigation. *Federal Bureau of Investigation*. https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure

FCC. (2024, December 5). *FCC Fact Sheet: Implications of Salt Typhoon attack and FCC response*. https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf

Federal Bureau of Investigation. (2022). *The China Threat*. Federal Bureau of Investigation. https://www.fbi.gov/investigate/counterintelligence/the-china-threat

Freeman, M. (2024, December 18). Breaking Down Salt Typhoon. *Armis*. https://www.armis.com/blog/breaking-down-salt-typhoon/

Forno, R. (2024, December 6). *What is Salt Typhoon? A security expert explains the Chinese hackers and their attack on US telecommunications networks*. UMBC; UMBC. https://umbc.edu/stories/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks/

Godefrey, Lester. *An Allied Perspective on Cyber*. Mar. 2022, p. 10, www.cia.gov/resources/csi/static/Article_Shape_or_Deter_Cyber-Espionage.pdf. Accessed 7 Sept. 2025.

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

Human Rights Report. (2024). *Technical Difficulties*. State.gov. https://www.state.gov/wp-content/uploads/2022/03/3136152_Brazil-2021-Human-Rights-Report.pdf?ref=hir.harvard.edu

Kapko, M. (2025, February 13). Salt Typhoon remains active, hits more telecom networks via Cisco routers. *CyberScoop*. https://cyberscoop.com/salt-typhoon-china-ongoing-telecom-attack-spree/

Katz, Eyal. “A Step-by-Step Guide to SS7 Attacks.” *FirstPoint*, 26 Jan. 2020, www.firstpoint-mg.com/blog/ss7-attack-guide/.

News, The Hacker. “Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks.” *The Hacker News*, 21 Feb. 2025, www.thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html

“NVD - CVE-2024-21887.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/CVE-2024-21887.

“NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical.” *National Security Agency/Central Security Service*, 27 Aug. 2025, www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/.

OWASP. “Buffer Overflow.” *Owasp.org*, 2021, owasp.org/www-community/vulnerabilities/Buffer_Overflow.

Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security*, *157*, 104606. https://doi.org/10.1016/j.cose.2025.104606

Psirt, Pan. “CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway.” *Palo Alto Networks Product Security Assurance*, 12 Apr. 2024, security.paloaltonetworks.com/CVE-2024-3400.

Ribeiro, A. (2025, July 17). DHS: Salt Typhoon hackers breached Army National Guard, exposing admin credentials and network diagrams. *Industrial Cyber*. https://industrialcyber.co/critical-infrastructure/dhs-salt-typhoon-hackers-breached-army-national-guard-exposing-admin-credentials-and-network-diagrams/

Rissman, K. (2025, September 4). *Chinese cyberattacks may have stolen personal data from you and every other American*. The Independent. https://www.independent.co.uk/news/world/americas/us-politics/chinese-cyberattacks-stolen-personal-information-b2820122.html

Sain, S. (2025, April 1). FTCN Replay: Cybersecurity Expert Warns of Government Vulnerabilities Following Salt Typhoon Attack. *Journal of Electromagnetic Dominance*. https://www.jedonline.com/2025/08/04/ftcn-replay-cybersecurity-expert-warns-of-government-vulnerabilities-following-salt-typhoon-attack/

Sanger, D. E., Barnes, J. E., Barrett, D., & Goldman, A. (2024, November 23). Emerging Details of Chinese Hack Leave U.S. Officials Increasingly Concerned. *The New York Times*. https://www.nytimes.com/2024/11/22/us/politics/chinese-hack-telecom-white-house.html

Sanger, D. E., & Landler, M. (2024, March 25). U.S. and Britain Accuse China of Cyberespionage Campaign. *The New York Times*. https://www.nytimes.com/2024/03/25/us/politics/china-hacking-us-sanctions.html

Salt typhoon. Salt Typhoon, Group G1045 | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/groups/G1045/

Sayegh, E. (2025, August 30). *U.S. And Allies Declare Salt Typhoon Hack A National Defense Crisis*. Forbes. https://www.forbes.com/sites/emilsayegh/2025/08/30/us-and-allies-declare-salt-typhoon-hack-a-national-defense-crisis/

Schappert, S. (2025, August 27). *Chinese-backed Salt Typhoon tops list of international threats in latest cybersecurity advisory*. Cybernews. https://cybernews.com/security/international-cybersecurity-advisory-chinese-salt-typhoon-nation-state-threats/

US Foreign Intelligence Surveillance Court. (2025). *About the Foreign Intelligence Surveillance Court | Foreign Intelligence Surveillance Court | United States*. https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

USA, Australia, Canada, & New Zealand. (2025, September). *CSA Countering China State Actors Compromise of Networks*.

Viswanatha, A., & Krouse, S. (2025, August 27). *Chinese Spies Hit More Than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals*. The Wall Street Journal. https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f

Volz, D. (2025, April 10). *Exclusive | In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks*. The Wall Street Journal. https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb