Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume II, 115-122

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

Dimitar Dimitrov
Nikola Vaptsarov Naval Academy
IT Department
Varna, Bulgaria
dimitar@nvna.bg

Evgeni Andreev
Nikola Vaptsarov Naval Academy
IT Department
Varna, Bulgaria
e.andreev@naval-acad.bg

***Abstract* – China's strategic competition in cyberspace has evolved beyond traditional espionage, adopting a more aggressive posture that integrates cyber sabotage as a critical tool of statecraft. This paper examines the activities of the state-sponsored hacking groups Volt Typhoon and Salt Typhoon, highlighting its transition from intelligence gathering to disruptive cyber operations against critical infrastructure. By leveraging Living off the Land Binaries (LOLBins) and exploiting vulnerabilities in SOHO network devices, Volt Typhoon has demonstrated an ability to maintain persistent access while evading detection. The group's infiltration of U.S. military networks in Guam is analysed as a case study reflecting Beijing's broader strategic ambitions in the Indo-Pacific. The findings suggest that China's cyber doctrine is shifting toward pre-positioning for offensive capabilities, enabling covert battlefield preparation in anticipation of geopolitical escalations. The study underscores the necessity for proactive cybersecurity measures, advanced threat intelligence sharing and international collaboration to counter the emerging threats posed by China's evolving cyber warfare strategy**

Keywords* – *China, Salt Typhoon, Strategic competition, Volt Typhoon

I. INTRODUCTION

The contest for geopolitical dominance in the 21st century is increasingly taking place in cyberspace, where states are competing for strategic advantage beyond traditional military and economic domains. The People's Republic of China has now positioned itself at the forefront of this competition, using cyberspace not only as a tool for intelligence gathering, but also as a domain for the consolidation of power, enforcement and disruption. In the context of strategic competition [1] in which the US and China are engaged in a strategic competition for technological, military and economic supremacy, cyber operations have become a vital tool of statecraft. The evolution of Chinese cyber activities from espionage to pre-staging disruptive attacks signals a fundamental shift in how China is envisioning warfare.

Strategic competition is broadly defined as the ongoing competition among great powers to shape global order, technological standards and military balance without direct kinetic conflict. Historically, great power competition has revolved around economic influence, military alliances and ideological struggles. Today, cyberspace has become the newest and most contested area in this struggle. The United States, which has long enjoyed technological superiority, now faces an assertive China that seeks to challenge US dominance through systematic cyber interventions, technological acquisitions and digital coercion. Volt Typhoon and Salt Typhoon serve as examples of this shift, as they are not simply intelligence gathering missions, but pre-emptive measures designed to embed China's cyber capabilities into critical infrastructure, ensuring its influence in times of crisis. The PRC's ability to penetrate and maintain constant access to telecommunications networks, energy grids and defence infrastructure represents an unprecedented escalation in digital statecraft.

The activities of Volt Typhoon underscore China's increasing reliance on the prepositioning of cyber assets in U.S. critical infrastructure as a means of deterrence and coercion. Unlike conventional cyberespionage campaigns, which primarily seek to obtain intelligence for diplomatic, military, or economic purposes, Volt Typhoon operates with the clear goal of infiltrating vital national infrastructure while remaining undetected for long periods

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol2.8618

of time. The Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency CISA concluded that Volt Typhoon is preparing for future geopolitical contingencies by gaining continued access to U.S. energy, water and transportation systems. By exploiting vulnerabilities in small office and home office routers and using "living off the land" techniques to blend into legitimate network traffic, the group ensures it can carry out crippling cyberattacks with minimal warning. This operational strategy suggests that the PRC views cyberspace not only as an area for intelligence gathering, but also as an overtaking battlefield where attacks on infrastructure can serve to multiply forces during conflict. At the same time, Salt Typhoon demonstrates a different but equally troubling strategic focus on the telecommunications sector. In late 2024, US intelligence confirmed that Salt Typhoon had successfully compromised nine major US telecommunications providers, including AT&T and Verizon. This breach allowed Chinese agents to gain access to routing infrastructure, manipulate network traffic and potentially intercept sensitive government and military communications. Unlike previous cyberattacks aimed at stealing intellectual property, Salt Typhoon represents an offensive capability designed to disrupt or degrade U.S. command and control structures in a crisis scenario. The implications of such a capability extend beyond immediate national security concerns if unchecked, it could allow China to paralyze U.S. military responses, delay crisis coordination and even manipulate information flows during wartime. This approach is consistent with broader Chinese military doctrine, which views cyber operations as an integral part of modern warfare capable of achieving strategic objectives without direct military confrontation.

The broader strategic context of these operations must be understood within China's long-term geopolitical ambitions[2]. The PRC's cyber doctrine is deeply intertwined with its goals of regional hegemony, particularly in the Indo-Pacific where it seeks to challenge US military and economic influence. A U.S. Department of Defence 2024 report identifies cyber warfare as a key enabler of China's broader "smart war" strategy, in which cyber, artificial intelligence and information dominance are used to neutralize adversaries before kinetic engagements begin. This doctrine is particularly relevant in scenarios such as the Taiwan contingency, where cyber operations targeting U.S. and allied infrastructure can delay or disrupt military force mobilization efforts. The activities of Volt Typhoon and Salt Typhoon are fitting right into this framework, reinforcing the idea that China is methodically building a cyber battlespace that can be activated at a moment's notice.

This paper examines how China's cyber strategy, as reflected in the activities of Volt Typhoon and Salt Typhoon, represents a paradigm shift toward a more offensive and strategically disruptive posture. By analyzing their methods, objectives and implications, this study will explore how the PRC's cyber operations extend beyond espionage to battlefield preparation, coercion and strategic deterrence. Ultimately, understanding this shift is critical for developing robust cybersecurity policies and international countermeasures to mitigate the risks posed by China's evolving cyber warfare strategy.

II. Materials and Methods

China's cyber strategy is embedded deeply within the broader national security framework [3], guided by the active defence doctrine and reinforced by the military-civilian fusion model. In contrast to other countries that rely primarily on specialized cyber units within their military or intelligence services, China has created a vast ecosystem in which government, corporate and academic entities act in synergy to develop its cyber capabilities. This approach ensures that civilian technological innovation directly supports China's cyberwarfare objectives by providing the Chinese Communist Party with an extensive infrastructure for cyber intelligence collection and offensive operations. The principle of active defence, a longstanding component of Chinese military doctrine, has been extended into the digital domain. It justifies preemptive cyber operations as a means to neutralize threats before they materialize. This philosophy is reflected in China's National Defence White Papers (2007, 2015, 2018) [4],[5], which expand state control over Internet governance, technology exports and corporate data practices. Unlike Western countries, where private companies typically operate independently of state directives, China obliges its corporations to comply with national security objectives, effectively turning private firms into extensions of state intelligence operations.

Key evidence of this doctrine is China's growing dominance of global technology markets. Through its quasi-monopoly control over the production of telecommunications equipment [6], semiconductors and surveillance technologies, China has infiltrated the digital infrastructure of governments, businesses and military institutions around the world. This not only strengthens Beijing's economic and technological influence, but also creates security risks, as widely used hardware and software produced in China may contain backdoors that could be exploited in future conflicts.

A. Integration of Cyber Operations into National Security

The People's Republic of China does not perceive cyber operations exclusively as a means of economic and technological advancement, rather, they constitute an integral component of its national security doctrine [7]. In contrast to conventional warfare, where conflicts are overt and direct, cyberwarfare offers the PRC low-risk, high-payoff avenues to achieve its strategic objectives without immediate retaliation. Legislation such as the 2017 Cybersecurity Law and the National Intelligence Law grants intelligence agencies significant authority to compel private companies to cooperate, stipulating that all Chinese companies both domestic and foreign must share data with the government upon request. This legal framework enables the CCP to utilize prominent technology companies like Huawei, Hikvision and ZTE as platforms

for intelligence gathering and covert cyber operations. Through its control over global technology supply chains, Beijing exerts influence over nations that rely on Chinese-built digital infrastructure, particularly in the developing world. The expansion of Chinese 5G networks, cloud services and telecommunications infrastructure in these regions not only enhances Beijing's economic leverage but also provides potential access to sensitive communications data. These security concerns have prompted bans and restrictions on Chinese technology companies, particularly in the United States and Europe. The US government has expressed concerns about the potential risks associated with Chinese-made telecommunications equipment, citing the possibility of espionage and cyber sabotage in future conflicts. Hidden vulnerabilities in Chinese equipment could be activated to disrupt critical infrastructure, further escalating geopolitical tensions.

Beyond infrastructure control, China employs cyber operations to steal intellectual property, disrupt economies and manipulate global information ecosystems. Cyber intrusions targeting foreign research institutions, defence contractors and government agencies have resulted in the exfiltration of vast amounts of classified data. These operations grant China long-term strategic advantages in critical fields such as military technology, artificial intelligence (AI), quantum computing and semiconductor development. By systematically targeting emerging technologies, Beijing accelerates its own innovation while simultaneously undermining the technological superiority of its geopolitical rivals.

China’s cyber strategy also plays a pivotal role in its territorial disputes and regional power projection [8]. Cyberattacks against Taiwan’s critical infrastructure have grown in frequency and sophistication, signalling Beijing’s readiness to integrate digital warfare into its broader strategy for asserting territorial claims. These operations extend beyond espionage, often involving distributed denial-of-service (DDoS) attacks, supply chain compromises and malware injections aimed at destabilizing Taiwan’s political and economic stability.

Similarly, China’s cyber operations target U.S. allies in the Indo-Pacific, aiming to disrupt regional security cooperation and preempt countermeasures against Beijing’s expansionist ambitions. Cyberespionage campaigns against Japan, Australia and India have sought to infiltrate defence networks, exploit critical infrastructure vulnerabilities and extract intelligence on military alliances. These activities align with China’s broader strategy of undermining U.S.-led security frameworks while expanding its sphere of influence in the Indo-Pacific. China's integration of cyber operations into its geopolitical strategy reflects a comprehensive approach to digital dominance, wherein cyber capabilities serve as both an offensive weapon and a strategic deterrent. By leveraging its technological infrastructure, espionage networks and cyber sabotage capabilities, China continues to reshape global power dynamics in its favor, challenging traditional military and economic paradigms in the process.

B. Information Warfare and Cyber Intelligence: A Tool for Strategic Competition

China’s cyberwarfare strategy is not merely a means of espionage or digital disruption it is a key instrument of strategic competition, designed to undermine rivals, shape global narratives and expand Beijing’s geopolitical influence. The Chinese Communist Party views information dominance [9] as a critical pillar of national power projection, recognizing that controlling digital ecosystems allows China to manipulate foreign public perception, disrupt adversary decision-making and neutralize political opposition. Unlike traditional military engagements, where power is projected through force, China uses cyberspace as a strategic battleground, integrating cyber intelligence, disinformation campaigns and covert digital operations to erode the economic, political and military advantages of its global competitors. Through persistent cyber intrusions and information warfare tactics, China seeks to gain leverage over adversaries, preempt security countermeasures and strengthen its geopolitical positioning without triggering conventional conflict.

China’s cyber intelligence operations began with low-level disruptions, such as website defacements and digital propaganda. However, by the early 2000s, Beijing transitioned to large-scale cyber espionage campaigns aimed at extracting high-value intelligence from rival nations. The campaign resulted in the theft of terabytes of classified data, including military intelligence and strategic defence plans, allowing China to reverse engineer Western military capabilities. Advanced technological blueprints, accelerating China’s development in key sectors such as aerospace, cybersecurity and artificial intelligence. Also governmental and diplomatic intelligence, granting Beijing a competitive edge in global negotiations and security policymaking.

China’s cyber intelligence efforts are closely linked to its broader strategy of technological and economic competition. Rather than relying solely on military strength, China leverages cyber operations to achieve dominance in critical industries, weaken economic competitors and influence global governance structures. Key areas where cyber intelligence fuels China’s strategic ambitions include economic and Industrial Espionage – Chinese cyber actors systematically target foreign corporations, research institutions and critical supply chains to steal trade secrets, intellectual property and technological innovations. This approach accelerates China’s domestic industrial growth while simultaneously undermining Western economic superiority. Energy and Infrastructure Disruption – China has increasingly focused on compromising energy grids, transportation networks and supply chains, positioning itself to disrupt the infrastructure of rival nations in times of geopolitical tension. Electoral and Political Manipulation – Chinese cyber operatives engage in disinformation campaigns and social media influence operations to shape public discourse, weaken democratic institutions and foster political instability in competitor states.

III. RESULTS AND DISCUSSION

A defining example of China's shift from cyber espionage to disruptive cyber warfare is Volt Typhoon[10], a state-sponsored hacking group that exemplifies Beijing's evolving doctrine of cyber pre-positioning and infrastructure infiltration. First identified in 2021 by Palo Alto Networks' Unit 42, Volt Typhoon, also known as Vanguard Panda, DEV-0391, UNC3236, Voltzite and Insidious Taurus, operates with an advanced level of stealth, focusing on embedding itself within critical infrastructure while maintaining long-term persistence. Unlike traditional cyber actors that seek immediate data exfiltration, Volt Typhoon's approach is one of strategic latency, ensuring that compromised systems remain under its control for years, ready for potential activation in times of geopolitical escalation.

The group's techniques were further analysed by Microsoft's Threat Intelligence Division, which confirmed its use of LOLBins, a strategy that enables the execution of malicious commands using legitimate system tools, avoiding the need to introduce foreign code that might trigger security alerts [11]. Additionally, Volt Typhoon employs botnet networks to obfuscate its command and control traffic, routing malicious activity through compromised devices particularly small office/home office routers. This makes attribution difficult and allows the group to blend into regular internet traffic, complicating detection efforts by cybersecurity professionals. These methods have allowed Volt Typhoon to infiltrate U.S. critical infrastructure, targeting communications, energy grids and transportation systems, sectors essential for national security and military operations. The Five Eyes intelligence alliance has repeatedly raised alarms about Volt Typhoon's activities. Reports from May 2023 and February 2024 [12], [13] indicate that the group has maintained persistent access to U.S. infrastructure for over five years, raising concerns about its ability to disrupt essential services at a moment's notice. The group's strategic targeting suggests that its operations are not opportunistic but carefully orchestrated, designed to position China with cyber leverage over adversaries by embedding itself within networks long before conflict arises.

A key example of Volt Typhoon's strategic importance was its infiltration of U.S. military networks in Guam, a critical base for Indo-Pacific operations. On May 24, 2023, Microsoft [14] disclosed evidence of Volt Typhoon malware found within the network infrastructure linked to U.S. Department of Defence operations in Guam, triggering immediate concerns among policymakers. Guam serves as a major hub for U.S. military readiness in the Indo-Pacific, playing a vital role in power projection, logistics and rapid response operations, particularly concerning Taiwan. While forensic investigations did not reveal immediate sabotage, the intrusions pointed to intelligence gathering and strategic mapping of critical communication networks. By understanding the communication flows, system architecture and operational dependencies of U.S. military infrastructure in Guam, Volt Typhoon's operators were likely laying the groundwork for future offensive actions [15], ensuring that in the event of a conflict, China could disrupt or neutralize essential command and control systems. This prepositioning strategy reflects Beijing's shift towards an offensive cyber posture, where cyber operations are not just about data theft, but about neutralizing adversaries capabilities before conventional hostilities begin.

One of the defining characteristics of Volt Typhoon is its ability to remain undetected [16] for extended periods. This is achieved through a combination of stealth tactics, proxy networks and unconventional attack methods. Rather than relying only deploying signature-based malware that can be flagged by security software, Volt Typhoon leverages native Windows administration tools, making its activities appear as routine system processes. These include WMIC (Windows Management Instrumentation Command-line) used to collect system information and execute administrative commands. PowerShell which exploited for executing scripts that evade detection by security tools. NTDSutil utility used to interact with Active Directory services, enabling the extraction of domain credentials. Netsh used for port forwarding and traffic redirection, enabling remote access without triggering security alerts. Additionally, Volt Typhoon utilized the KV botnet, a sophisticated malware tool that allows operators to route traffic through compromised devices, obscuring their true origin. Volt Typhoon's operational methodology [17] is deeply rooted in advanced cyber intrusion techniques designed to maintain stealth, persistence and long-term access to compromised systems. A key component of its tactics, techniques and procedures revolves around the use of built-in system binaries and administrative tools to evade detection while achieving its operational objectives. By leveraging non-administrative credentials, Volt Typhoon operators can execute commands directly via the command line interface (T1059.003) and those avoiding endpoint security solutions that typically monitor for anomalous script execution.

One of the primary objectives of Volt Typhoon's post-exploitation phase is the collection and exfiltration of high-value authentication credentials. This is achieved by targeting Active Directory domain controllers, where the ntds.dit file resides. This file contains hashed passwords and authentication data for all domain accounts, making it an invaluable resource for attackers seeking to escalate privileges and pivot within the network (T1003.003). However, given that the ntds.dit file is typically locked and secured by system processes, Volt Typhoon employs shadow volume copies to create unauthorized duplicates of the file, bypassing standard security controls and enabling offline extraction and decryption. The manipulation of volume shadow copies is a well-documented technique that allows adversaries to circumvent direct access restrictions and obtain sensitive credentials without alerting active security monitoring systems.

Beyond credential theft, Volt Typhoon demonstrates a sophisticated understanding of network traffic

manipulation and lateral movement. The actor employs port forwarding and proxy techniques (T1090) to facilitate covert remote access to compromised hosts. Specifically, Volt Typhoon utilizes the Netsh utility, a built-in Windows networking tool, to modify firewall configurations and establish persistent tunnels between infected machines. Through the port proxy add command, the adversary can redirect incoming connections to designated ports, effectively obfuscating the true origin of their malicious traffic while maintaining a low forensic footprint. This allows Volt Typhoon to maintain persistent remote access without triggering traditional intrusion detection systems or endpoint detection and response (EDR) solutions that rely on behavioural analysis of anomalous network traffic.

A. Salt Typhoon

Following Volt Typhoon's extensive infiltration of critical infrastructure, a second Chinese state-sponsored hacking group codename Salt Typhoon [18] exemplifies the People's Republic of China's focus on compromising telecommunications systems for both espionage and potential sabotage. Salt Typhoon is the name most widely used to describe the group, assigned by Microsoft, though various cybersecurity vendors have identified the same actor under different designations: Earth Estrie (Trend Micro), Ghost Emperor (Kaspersky Lab), FamousSparrow (ESET), and UNC2286 (Mandiant). The group is believed to operate under the auspices of China's Ministry of State Security (MSS).

Salt Typhoon's primary hallmark is its systematic and targeted campaign against major U.S. telecommunications providers [19], [20], demonstrating a highly refined ability to exploit core network vulnerabilities for both next level intelligence collection and potential operational disruption. The group's focus on high-value telecom carriers, including T-Mobile, AT&T, Verizon, and Lumen Technologies, suggests a deliberate strategy aimed at infiltrating critical communications infrastructure at multiple levels. By breaching both commercial and enterprise networks, Salt Typhoon has gained the capability to manipulate sensitive communication flows [21], [22], monitor government and law enforcement traffic, and potentially stage future cyber-sabotage operations. These breaches not only signal the growing sophistication of China's cyber operations but also underscore the pressing need for strengthened security measures across the telecommunications sector.

The infiltration of major telecom providers by Salt Typhoon represents a significant escalation in China's state-sponsored cyber operations, shifting from traditional intelligence gathering to direct threats against national security infrastructure. Investigations indicate that Salt Typhoon successfully compromised core routing infrastructure, network management systems, and customer databases, granting attackers the ability to monitor, intercept, manipulate, and potentially disrupt U.S. communications. Reports from federal cybersecurity agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI), confirm that these breaches extended to the interception of sensitive government and law enforcement surveillance data, further emphasizing the far-reaching national security implications of these attacks.

Salt Typhoon's attack methodology relies on exploiting known vulnerabilities in telecommunications hardware and software, particularly within Cisco's IOS XE network operating system. The group has been observed leveraging CVE-2023-20198 and CVE-2023-20273 [23], both of which allow unauthorized attackers to execute arbitrary commands with administrative privileges. Once inside the network, the attackers deploy living-off-the-land techniques, abusing built-in diagnostic and management tools like SNMP, Telnet, and SSH to move laterally within compromised environments. By avoiding the introduction of foreign binaries or malware, Salt Typhoon ensures that traditional endpoint detection and response (EDR) systems are unable to flag its activity as anomalous, thereby prolonging its presence within victim networks.

The impact of these breaches extends far beyond data theft. With control over routing infrastructure, Salt Typhoon can reroute traffic, perform deep packet inspection, and even selectively drop or delay communications between government agencies, military units, and emergency response teams. This capability poses a direct threat to U.S. national security, as the ability to manipulate real-time communications can degrade crisis response efforts, disrupt logistics coordination, and even compromise battlefield decision-making processes. Further investigations have revealed that Salt Typhoon's access extends to telecom-managed infrastructure critical to the U.S. Department of Defence, law enforcement, and intelligence operations. Some of the compromised networks include those handling secure government communications, raising concerns that adversaries may have gained insights into classified or sensitive government directives. The potential for adversaries to manipulate call metadata, intercept sensitive conversations, or even inject misinformation into communication channels adds another layer of risk to national security. Intelligence reports indicate that Salt Typhoon targeted specific individuals in government and military leadership, suggesting a more sophisticated and selective approach to intelligence collection.

Beyond the U.S., allied nations have also reported increased activity linked to Salt Typhoon, particularly in Europe and Asia. Several European Union member states have flagged similar telecom intrusions, raising concerns that the group is conducting a coordinated, global campaign to compromise Western telecommunications infrastructure. Reports from Germany, France, and the Netherlands indicate that state-sponsored hackers have targeted telecom firms responsible for handling sensitive government communications, further demonstrating the widespread impact of Salt Typhoon's operations.

One of the most concerning aspects of Salt Typhoon's campaign is its ability to maintain long-term persistence within compromised networks. By modifying router

configurations, implanting secondary access mechanisms, and exfiltrating authentication credentials, the group ensures that its foothold remains intact even after initial remediation efforts. Security researchers have identified instances where Salt Typhoon re-entered previously secured networks by leveraging stolen administrative credentials, demonstrating the need for organizations to implement stronger access controls and multi-factor authentication to mitigate the risk of re-compromise.

The scale of Salt Typhoon's operations suggests a well-funded and highly coordinated effort backed by the Chinese government. Unlike traditional cybercriminal groups that focus on financial gain, Salt Typhoon's objectives align with broader geopolitical strategies aimed at undermining Western influence and enhancing China's strategic position in cyberspace. The integration of offensive cyber operations into China's military doctrine further emphasizes the role of groups like Salt Typhoon in future conflicts, where digital disruption of critical infrastructure can serve as a force multiplier alongside conventional military capabilities. This approach highlights a "long-game" strategy, aligning with what former NSA analyst Terry Dunlap has referred to as a component of China's "100-Year Strategy."

B. Implications for Global Cyber Competition

Salt Typhoon and Volt Typhoon's persistent infiltration into telecommunications, energy, and military networks signals a dramatic expansion of China's cyber battlespace. These operations are no longer limited to espionage but have evolved into strategic tools for pre-positioning within adversarial infrastructure, ensuring that China retains the ability to disable critical systems at will. The combined threat of these two APT groups has reshaped global cybersecurity paradigms, forcing Western governments to reevaluate their defensive postures and accelerate countermeasures. The Chinese strategy [24]of embedding cyber assets within critical infrastructure long before a crisis occurs provides a decisive advantage, enabling China to undermine adversarial capabilities and shape the operational environment in its favor.

The strategic significance of Volt Typhoon and Salt Typhoon lies in their complementary operational focus. While Volt Typhoon prioritizes access to energy grids, water utilities, and transportation networks, Salt Typhoon has infiltrated telecommunications infrastructure, granting China potential control over communication lines essential to military coordination and crisis response. This dual-pronged approach ensures that in the event of a geopolitical escalation, China can selectively disrupt key infrastructure components to weaken adversaries before physical hostilities begin. Such tactics mirror China's broader "smart war" strategy, in which cyber operations play a central role in shaping battlefield conditions and neutralizing threats before kinetic conflict erupts.

As these cyber threats continue to evolve, national security agencies worldwide are ramping up intelligence-sharing initiatives to counteract the expanding Chinese cyber presence. The United States, in coordination with its allies in the Five Eyes intelligence alliance, has intensified cybersecurity collaboration, issuing joint advisories and reinforcing defensive capabilities across telecommunications, defense, and critical infrastructure sectors. European nations, similarly affected by Chinese cyber operations, are integrating their cybersecurity frameworks with NATO's cyber defense initiatives, aiming to create a more resilient digital infrastructure capable of withstanding state-sponsored attacks.

Despite these countermeasures, the persistent nature of China's cyber intrusions highlights the weaknesses in traditional cybersecurity approaches. Standard defensive measures, such as firewalls and endpoint security solutions, have proven inadequate against the sophisticated, stealthy tactics employed by Volt Typhoon and Salt Typhoon [25]. The widespread use of living-off-the-land techniques, which allow attackers to exploit legitimate administrative tools rather than deploy detectable malware, has further complicated mitigation efforts. As a result, governments and private sector entities are increasingly turning to artificial intelligence-driven anomaly detection and behavioral analytics to identify and counteract these advanced threats in real time.

The evolution of China's cyber operations has significant implications for international law and cyber norms. While espionage has long been accepted as a standard state practice, the deliberate pre-positioning of cyber assets within adversarial infrastructure crosses into more aggressive territory, bordering on acts of war. This shift has prompted discussions within the United Nations and other international forums regarding the need to establish clearer rules of engagement for cyber conflicts. However, China's strategic use of plausible deniability hiding its operations behind layers of proxies and compromised infrastructure complicates attribution and response strategies, making it difficult for affected nations to take decisive action.

Beyond traditional cybersecurity concerns, the activities of Volt Typhoon and Salt Typhoon highlight the growing risks associated with digital supply chain vulnerabilities. Chinese influence over global telecommunications equipment manufacturing raises concerns that compromised hardware and firmware could be pre-infected with backdoors, providing China with remote access capabilities without requiring direct network breaches. The recent scrutiny of Chinese technology providers, such as Huawei and ZTE, underscores the urgent need for nations to diversify their supply chains and reduce reliance on potentially compromised hardware components.

Looking beyond espionage, Volt Typhoon and Salt Typhoon's operational playbook indicates a clear transition toward full-fledged cyber warfare assets. These groups have already demonstrated their ability to infiltrate and manipulate critical infrastructure; the next logical step is the execution of coordinated cyberattacks designed to paralyze adversary responses during conflict scenarios. In

a future military engagement, China could simultaneously disrupt power grids, sever communication links, and introduce disinformation into government systems, significantly impairing an adversary's ability to coordinate an effective defense. The potential for escalation into full-scale cyber warfare is a growing concern among defense analysts. Unlike conventional warfare, cyber conflicts lack clear thresholds for response, making it difficult to determine when an attack warrants military retaliation. This ambiguity increases the risk of miscalculation, as states struggle to attribute cyber incidents and calibrate their responses accordingly.

As the global cybersecurity landscape continues to evolve, nations must take decisive steps to mitigate the risks posed by state-sponsored cyber threats. The rise of Volt Typhoon and Salt Typhoon underscores the urgent need for proactive threat hunting, improved intelligence-sharing mechanisms, and stricter supply chain security standards. Without coordinated international efforts to counter China's expanding cyber capabilities, the world risks entering an era where cyber warfare becomes a routine element of geopolitical competition, with far-reaching consequences for global stability and security.

IV. Conclusions

The persistence and stealth of Volt Typhoon's operations suggest that China is no longer merely engaging in passive cyber espionage. Instead, it is actively positioning cyber assets within adversary infrastructure, ready to disable or degrade critical services in the event of conflict. This represents a fundamental shift in cyber warfare doctrine, where state-sponsored hacking groups do not simply steal information but prepare the digital battlespace for future engagements. The implications are clear - China is no longer deterred by traditional cyber norms and Volt Typhoon and Salt Typhoon operations suggest a growing willingness to explore offensive cyber capabilities that could disrupt power grids, sever communication lines and compromise military command structures. The paradigm shifts in cyber warfare from espionage to infrastructure pre-positioning underscores the need for enhanced cyber resilience, proactive threat intelligence sharing and offensive cyber deterrence measures.

As geopolitical tensions rise, the United States and its allies must act swiftly to secure critical infrastructure, develop real time threat mitigation strategies and ensure that Volt Typhoon's long-term persistence does not translate into a catastrophic vulnerability. Failure to do so could leave essential national security assets exposed, granting China a significant cyber advantage in future conflicts.

References

[1] K. He et al., "Understanding the dynamics of the Indo-Pacific: US–China strategic competition, regional actors, and beyond," International Affairs, vol. 96, no. 1, pp. 1–7, 2020. doi: 10.1093/ia/iiz242

[2] M. Kolton, "Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence," *The Cyber Defense Review*, vol. 2, no. 1, pp. 119–154, 2017. [Online]. Available: http://www.jstor.org/stable/26267405. [Accessed: Feb. 16, 2025].

[3] "Forward Persistence in Great Power Cyber Competition," Dec. 19, 2024. [Online]. Available: https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Lynch_CDRV9N3-Fall-2024.pdf. [Accessed: Feb. 16, 2025].

[4] "China's Military Strategy," May 27, 2015. [Online]. Available: https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm. [Accessed: Feb. 16, 2025].

[5] "The 2004 Chinese Defence White Paper," Mar. 18, 2005. [Online]. Available: https://rusi.org/publication/2004-chinese-defence-white-paper. [Accessed: Feb. 16, 2025].

[6] "SWJ Primer: Chinese Cyber Espionage and Information Warfare," Apr. 29, 2019. [Online]. Available: https://archive.smallwarsjournal.com/index.php/jrnl/art/swj-primer-chinese-cyber-espionage-and-information-warfare. [Accessed: Feb. 18, 2025].

[7] M. N. Mirza et al., "Conceptualising cyber sovereignty and information security: China's image of a global cyber order," *Webology*, vol. 18, no. 5, 2021. [Online]. Available: https://ssrn.com/abstract=4056104. [Accessed: Feb. 18, 2025].

[8] R. Creemers, "The Chinese conception of cybersecurity: A conceptual, institutional, and regulatory genealogy," *Journal of Contemporary China*, vol. 33, no. 146, pp. 173–188, 2023. doi: 10.1080/10670564.2023.2196508

[9] R. Creemers, "China's conception of cyber sovereignty: Rhetoric and realization," in *Governing Cyberspace: Behavior, Power, and Diplomacy*, pp. 107–142, 2020. [Online]. Available: https://ssrn.com/abstract=3532421. [Accessed: Feb. 18, 2025].

[10] "Volt Typhoon and the Disruption of the U.S. Cyber Strategy," Mar. 5, 2024. [Online]. Available: https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy. [Accessed: Feb. 18, 2025].

[11] "Chinese Hack Pushes Up Against Guardrails Intended to Manage U.S.-Chinese Strategic Competition," Feb. 6, 2024. [Online]. Available: https://www.bradley.com/insights/publications/2024/02/chinese-hack-pushes-up-against-guardrails-intended-to-manage-us-chinese-strategic-competition. [Accessed: Feb. 19, 2025].

[12]] "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," May 24, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a. [Accessed: Feb. 20, 2025].

[13] "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/. [Accessed: Feb. 20, 2025].

[14] "Volt Typhoon's future war," Mar. 14, 2024. [Online]. Available: https://blog.barracuda.com/2024/03/14/volt-typhoon-future-war. [Accessed: Feb. 20, 2025].

[15] "Eroding Global Stability: The Cybersecurity Strategies of China, Russia, North Korea, and Iran," Aug. 01, 2024. [Online]. Available: https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/. [Accessed: Feb. 20, 2025].

[16] "Threat Brief: Attacks on Critical Infrastructure Attributed to Insidious Taurus (Volt Typhoon)," Feb. 14, 2024. [Online]. Available: https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/. [Accessed: Feb. 20, 2025].

[17] "The Rise of Chinese APT Campaigns: Volt Typhoon, Salt Typhoon, Flax Typhoon, and Velvet Ant," Oct. 24, 2024. [Online]. Available: https://eclypsium.com/blog/the-rise-of-chinese-apt-campaigns-volt-typhoon-salt-typhoon-flax-typhoon-and-velvet-ant/. [Accessed: Feb. 21, 2025].

[18] "US Telecom Giants Under Siege: 'Salt Typhoon' Cyber Assault Linked to China," Oct. 15, 2024. [Online]. Available: https://cybelangel.com/us-telecom-salt-typhoon-cyber-assault-china/. [Accessed: Feb. 21, 2025].

[19] "Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications," Nov. 15, 2024. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF12798. [Accessed: Feb. 21, 2025].

[20] "Governments, Telcos Ward Off China's Hacking Typhoons," Dec. 11, 2024. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/governments-telcos-chinas-hacking-typhoons. [Accessed: Feb. 21, 2025].

[21] "US adds 9th telecom company to list of known Salt Typhoon targets," Dec. 27, 2024. [Online]. Available: https://therecord.media/nine-us-companies-hacked-salt-typhoon-china-espionage. [Accessed: Feb. 23, 2025].

[22] "RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers," Feb. 13, 2025. [Online]. Available: https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices. [Accessed: Feb. 23, 2025].

[23] H. T. Hung, "Exploring China's cyber sovereignty concept and artificial intelligence governance model: A machine learning approach," *Journal of Computational Social Science*, vol. 8, no. 24, 2025. doi: 10.1007/s42001-024-00346-8

[24] "Weathering the storm: In the midst of a Typhoon," Feb. 20, 2025. [Online]. Available: https://blog.talosintelligence.com/salt-typhoon-analysis/. [Accessed: Feb. 23, 2025].