NJCCIC

China-Linked Cyber Operations Targeting US Critical Infrastructure

THREAT ANALYSIS REPORT

MAY 2025

Cyber Threat Outreach & Partnerships Bureau

Table of Contents

Executive Summary

China is engaging in sustained cyber operations targeting US critical infrastructure to lay the foundation for future disruption of key lifeline services. Advanced persistent threat (APT) groups like Volt Typhoon, APT41, and Salt Typhoon are spearheading this activity and have demonstrated sophisticated capabilities to access and persist within critical systems, particularly across the communications, energy, water and wastewater, and transportation sectors. They conduct stealthy, long-term intrusions by leveraging legitimate account credentials, edge devices, and remote access tools to maintain persistence in targeted environments. Intelligence indicates that these and other Chinese state-sponsored threat actors are preparing to launch destructive cyberattacks during a conflict between the United States and China.

A recent US House Committee on Homeland Security hearing in March reinforced the threats associated with this activity. Bill Evanina, founder and CEO of the Evanina Group and former Director of the US National Counterintelligence and Security Center, testified: “Cyber breaches, insider threats, surveillance, and penetrations into our critical infrastructure have all been widely reported. Adding in [their] crippling stranglehold on so many aspects of our supply chain, and the result is a montage of domestic vulnerability of unacceptable proportions.”

The intrusions extend beyond intelligence gathering and intellectual property theft activities. Instead, these campaigns are tailored to surveil, infiltrate, and ultimately control the systems and networks they penetrate. China is likely to prioritize targeting critical infrastructure in the US to delay or inhibit the mobilization of military forces. The attacks could lead to widespread service disruptions, including the collapse of communications networks, power grid failures and blackouts, water shortages, and restricted transportation.

Recognition that Chinese state-sponsored actors have already gained footholds in key sectors of US infrastructure is growing, as public officials and private-sector leadership have raised concerns regarding this activity for several years. However, continued advancements in technology are expanding the attack surface. “Penetrating our networks, pre-positioning technological choke points, and profiting from those dependencies poses a direct challenge to US homeland security,” Evanina further warned.

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) assesses that the frequency and severity of these cyber operations will continue to increase as tensions in the Indo-Pacific region escalate and China seeks to undermine US resilience from within. This report outlines the tactics, actors, and implications of China-linked cyber activity

across four key sectors. It also provides strategic insight and operational guidance to counter the growing threat of pre-positioned, state-backed sabotage within America's most vital systems.

Geopolitical and Strategic Context: US-China Tensions and the Cyber War for Influence

Central to the intensifying cyber threat landscape between the United States and China are the broader geopolitical tensions that have emerged over the last two decades, and competing strategic interests have culminated in a dynamic where the cyber realm is increasingly viewed as a primary domain for conflict. Among the main sources of friction are territorial disputes in the South China Sea. China has expanded its military footprint by building artificial islands and asserting broad maritime claims that most of the international community considers illegal. At the same time, the trade war between the US and China has escalated in recent weeks, with competing tariffs and trade restrictions at the forefront of the Trump administration's economic strategy. Finally, and most importantly, the US continues to extend firm policy support to Taiwan, which China views as a violation of the "One China" principle.

Taiwan has long been considered a likely flashpoint for a future conflict between China and the United States. For the US, the island is essential to regional defense, forming part of the first island chain that anchors American alliances with Japan, South Korea, and the Philippines. To China, it represents a national reunification goal linked to the Communist Party's legitimacy. However, its economic prospects should not be ignored.

Taiwan is a critical node in the global semiconductor industry. It is home to the Taiwan Semiconductor Manufacturing Company (TSMC), which produces over 55% of the world's chips and nearly all advanced processors. Furthermore, approximately one-third of the annual global computing power originates from the island. The global chip industry and the assembly of all the electronic goods they enable depend almost entirely upon the Taiwan Strait. The island is, therefore, critical to determining the power strongholds of the future global economy.

If China were to gain control of this industry, it could also gain leverage over the global technology supply chain, paving the way for regional hegemony. China's power and influence would extend further into the Indo-Pacific, and this geopolitical shift would threaten US influence and security.

This context is essential when evaluating the scope of China's threat. Recent cyberattacks indicate a long-term campaign to reshape global power structures and destabilize adversaries like the United States. China's cyber posture is not strictly defensive or opportunistic. It is strategic, viewing disruption to critical infrastructure as a path to victory while avoiding direct military confrontation.

Risk Assessment and Analysis

The NJCCIC has assessed that China-linked cyber threats pose a sustained risk to US infrastructure, particularly within the lifeline sectors that form the foundation of national continuity and resilience. The communications, energy, water and wastewater, and transportation sectors face a high likelihood of targeting and a high potential impact if successfully compromised, placing them in the "Critical" risk tier. These domains form the cornerstones of everyday life and are integral to military readiness, emergency response, and civil, political, and economic stability.

In addition, the Financial Services and Government Services sectors face a medium likelihood of targeting and a high potential impact, placing them in the "High" risk tier. Successful cyberattacks against these domains could significantly disrupt economic stability and shake public confidence.

Chinese state-sponsored cyber operations are expected to increase with escalating geopolitical tensions. The NJCCIC anticipates that these threats will continue to evolve in scale and sophistication. Critical infrastructure organizations should view this threat activity as a persistent risk.

Risk Matrix

SECTOR	LIKELIHOOD	IMPACT	RISK LEVEL
ENERGY	HIGH	HIGH	CRITICAL
COMMUNICATIONS	HIGH	HIGH	CRITICAL
WATER & WASTEWATER	HIGH	HIGH	CRITICAL
TRANSPORTATION	HIGH	HIGH	CRITICAL
FINANCIAL	MEDIUM	HIGH	HIGH
GOVERNMENT	MEDIUM	HIGH	HIGH

This matrix reflects the NJCCIC's current strategic risk assessment, which is based on ongoing intelligence collection, observed threat actor behavior, and known vulnerabilities across these sectors. It is intended to guide risk prioritization and resource allocation for defensive measures across public and private sector partners.

Communications Sector

Overview

The communications sector is fundamental to society. It enables information delivery and communication and serves as a key intelligence resource. Chinese state-sponsored APT groups have consistently targeted this sector as part of their campaign to disrupt US critical infrastructure. The communications domain comprises public and private telecommunications infrastructure, including internet service providers (ISPs), mobile networks, satellite communications systems, undersea cable networks, and cloud systems. Cyber operations in this space are, therefore, highly strategic. Attacks typically combine advanced technical expertise with a long-term emphasis on maintaining persistence, and recent China-linked cyber activity reveals a focused effort to compromise the communications sector.

Tactics, Techniques, and Procedures

Communications service providers operate a broad attack surface that includes data centers, network appliances, customer portals, and more. Some providers use public-facing systems, which threat actors can regularly scan to identify a point of access. Various tactics are used when launching attacks, and in many cases, unpatched devices or valid account credentials serve as the initial entry point. Known vulnerabilities in edge devices and remote access systems, such as Fortinet FortiOS, Microsoft Exchange, and Citrix Gateway, are commonly exploited; however, threat actors may also use passwords compromised in previous attacks.

Once inside a network, the threat actors rely on living-off-the-land (LoTL) techniques to extract sensitive data and establish and maintain footholds that can be leveraged later. They have been observed abusing legitimate administrative tools to move laterally, conduct reconnaissance, and avoid detection while blending into regular activity. This approach minimizes their footprint and reduces the likelihood of detection by traditional security tools.

Credential and data theft are key elements of their post-compromise activity. Threat actors extract credentials from memory using tools like Mimikatz or subtle techniques such as keylogging and token theft. With these legitimate credentials, attackers can move laterally

across administrative domains and impersonate network engineers or administrators, providing them with access to conduct surveillance and harvest sensitive data, or even shut down networks.

Recent and Notable Activity

Cyber activity against the communications sector has increased significantly over the last few years, with most campaigns conducted by APT groups. These groups are actively engaged in infiltration and intelligence-gathering efforts to gain persistent access to infrastructure that could be disrupted or disabled during a future conflict. Volt Typhoon and Salt Typhoon are two notable threat actors targeting this industry. Both groups use valid compromised account credentials and exploit vulnerabilities to gain initial access, then leverage "living-off-the-land" techniques to evade detection while performing strategic reconnaissance and pre-positioning activities. These and other APT groups may utilize sophisticated cyber techniques to degrade or destroy communications capabilities.

In 2023, Volt Typhoon compromised telecom systems in Guam, gaining access through unpatched edge devices and stealthily maintaining persistence to conduct reconnaissance. In early 2024, Salt Typhoon exploited vulnerabilities in telecom infrastructure to proxy malicious traffic, obscure operational command-and-control (C2), and stage within major US telecom providers. These intrusions highlight the shift toward strategic pre-positioning and active misuse of communications infrastructure to support broader campaigns.

Implications and Impact

A large-scale cyberattack against the US communications sector would have an immediate impact, with cascading effects that could destabilize other critical lifeline sectors. Communications infrastructure enables the real-time information flow across government, military, commercial, and civilian domains. Service disruptions would significantly affect nearly every aspect of daily activity in the United States.

At the operational level, an attack could disable mobile networks, satellite communications, ISPs, or undersea cable infrastructure. Interruptions in service would compromise everything from 911 emergency call routing and air traffic communications to financial transactions and remote work capabilities. Millions of people would lose access to vital information. Furthermore, coordination efforts with other sectors would break down, response efforts would stall, and recovery timelines would lengthen.

The United States military would also face challenges due to their impaired situational awareness. American forces would be incapable of mobilizing quickly or coordinating with

allies, particularly with NATO partners and the Five Eyes alliance. Intelligence sharing and secure communication would be greatly reduced. As a result, the US national defense posture would begin to deteriorate.

Economically, the consequences could be devastating. The communications sector supports core operations for nearly every major industry. A disruption could bring down financial markets, shut down banking systems, interfere with logistics platforms, and halt cloud-based services. Losses from even a short-term outage would be substantial, and the reputational damage to service providers could linger far longer.

The impact could be severe for civilians as well, isolating communities across the country. Key services that rely on real-time communication, including ambulance dispatch, fire and rescue, and public alert systems, may be cut off immediately. Logistical networks for food distribution, fuel supply, and commercial transport could also be disrupted. During an extended outage, public panic and misinformation would likely surge without reliable communication channels.

Risk Assessment

The NJCCIC has assessed the communications sector as a critical risk due to its broad exposure to foreign cyber threats and essential role in supporting national security, emergency response, and daily public and private-sector operations. Both the likelihood and potential impact of a successful cyberattack are considered high. This assessment is based on persistent adversary access across the sector, including long-term footholds established by Chinese state-sponsored threat actors. Ongoing exploitation of technical vulnerabilities, particularly in edge devices, remote access infrastructure, and legacy telecom equipment, combined with inconsistent cybersecurity practices and insufficient network segmentation, increases the probability of disruption. A compromise could have cascading ramifications due to the sector's function as the connection between other critical infrastructure domains.

Energy Sector

Overview

The energy sector is critical for preserving the well-being of communities across the United States, providing electricity, oil, natural gas, and renewable energy. Chinese state-sponsored APT groups have long viewed this sector as a priority target due to its strategic value. The energy domain is deeply integrated with other critical infrastructure and encompasses power generation facilities, electrical grids, oil and gas pipelines, emergency

management systems, and fuel logistics. China-linked cyber campaigns against this sector are calculated and prioritize long-term system access. Threat actors have repeatedly demonstrated interest in compromising environments that govern the flow of electricity and fuel, likely intending to disrupt key functions during a geopolitical crisis.

Tactics, Techniques, and Procedures

The energy sector functions across a complex infrastructure and operates a wide range of connected technologies. This technology includes legacy systems, industrial control systems (ICS), public-facing supervisory control and data acquisition (SCADA) interfaces, and more. Threat actors routinely scan the web to identify misconfigured or outdated assets that offer an initial entry point. They employ various tactics when launching their attacks, and in many cases, unpatched devices or valid account credentials serve as the initial entry point. Vulnerabilities in common systems like Fortinet, SonicWall, and Citrix frequently serve as points of access. Compromised passwords also provide an avenue in.

Threat activity in the energy domain is not limited to utility companies. This sector relies on contracted service providers for everything from system maintenance to regulatory compliance, and APT groups have increasingly targeted third-party partners. These vendors are often provided with administrative credentials or VPN access into core network environments, which threat actors can leverage to bypass perimeter defenses.

After gaining system access, the threat actors employ LoTL tactics to conduct their activities. They rely on native tools to move laterally and establish persistence while blending in with regular administrative activity and network traffic. These techniques enable them to extract sensitive data and conduct reconnaissance without triggering antivirus or endpoint detection software.

Credential theft plays a key role in these intrusions. Threat actors often use tools like Mimikatz to extract passwords and authentication tokens directly from system memory, which can be used to impersonate administrators, escalate privileges, and access systems that manage grid operations and fuel logistics. In many environments, this access enables lateral movement from IT networks into OT domains, where outdated control systems, often lacking modern cybersecurity controls, can be manipulated to disrupt energy delivery.

Threat actors may also deploy malware that is difficult to detect and capable of surviving reboots or patching. Backdoors like ShadowPad or even custom variants embedded in software updates allow them to quietly maintain access while communicating over ports and mimicking expected traffic patterns.

Recent and Notable Activity

Cyber operations against the US energy sector have steadily increased in scope and sophistication, with APT groups demonstrating a clear intent to compromise critical infrastructure supporting electric power, fuel distribution, and grid operations. APT41 and Volt Typhoon are among the groups most frequently associated with targeting energy systems. They often begin by exploiting vulnerabilities in ICS/SCADA environments and vendor-managed access points and escalate access through credential theft and privilege abuse. Once inside, they deploy stealthy persistence mechanisms and leverage native tooling to move laterally into industrial control environments. These tactics enable adversaries to pre-position within systems essential to energy reliability and potentially degrade or disable them during a crisis.

In 2021, the Colonial Pipeline ransomware attack, while criminal in nature, exposed systemic weaknesses in fuel distribution resilience. More recently, Volt Typhoon has been observed conducting reconnaissance and pre-positioning within energy infrastructure, including electric utilities and fuel logistics systems, using compromised credentials and stealthy remote access techniques.

Implications and Impact

A widespread cyberattack targeting the US energy sector would immediately threaten national security, economic stability, and civilian welfare, and the effects would ripple quickly. This sector is interwoven with every other critical infrastructure domain and supports virtually all aspects of modern life, from powering hospitals and water treatment plants to enabling military activity and digital communication. Any disruption to its operations would have severe consequences.

The most direct implication would be the loss of electric power that halts industrial activity and public services. These outages would upend daily life for millions of Americans. Water treatment facilities would be unable to operate, hospitals would have to rely on backup generators to provide care, and financial systems would risk downtime or data corruption. Natural gas pipelines or oil distribution networks could also be impacted. Fuel would be in short supply, limiting transportation and supply chains.

The US military would also be impeded. An extensive cyberattack could disrupt power supplies to military bases that rely on stable energy resources for operations, communication, and defense systems. In a national emergency, even short-term outages

could delay response times. Even if military sites remain operational, adversaries may exploit interdependencies, like private sector energy suppliers supporting defense contractors, to create pressure points.

The economic impact of a cyberattack on the energy sector would be substantial. Fuel shortages would interrupt supply chains, driving up energy prices and stalling activity across multiple industries. Market volatility could increase dramatically as production output drops. Industrial regions that rely heavily on the energy sector would be hit especially hard. Local economies would tip downward, contributing to wider national economic strain.

A successful compromise would also affect the well-being of civilians. Hospitals, water treatment utilities, and communication systems could shut down, and manufacturing plants, transportation systems, and supply chain networks would grind to a halt. Regional blackouts would generate panic and undermine confidence in government response. At the same time, prolonged outages or fuel shortages could be life-threatening, leading to civil unrest.

Risk Assessment

The NJCCIC has assessed the Energy sector as a critical risk due to its high exposure to state-sponsored cyber threats and its foundational role in powering essential services across all critical infrastructure domains. Both the likelihood and potential impact of a successful cyberattack are considered high. This determination is based on persistent adversary access within ICS and SCADA environments, particularly through long-term intrusions by Chinese APT groups seeking to establish pre-positioned footholds. The expansion of smart grid infrastructure and distributed energy systems have introduced new access points, increasing the attack surface across the sector. Unpatched systems, poor network segmentation between it and OT environments, and weak cybersecurity practices further compound these risks.

Water and Wastewater

Overview

The Water and Wastewater sector ensures the availability of safe drinking water and wastewater treatment to protect communities and the environment. This sector also supports other critical infrastructure, including healthcare, agriculture, and energy. Chinese state-sponsored APT groups have shown a growing interest in targeting US water facilities, leveraging many of the same techniques used in campaigns against other industries but with adaptations specific to the water and wastewater domain. This infrastructure includes

municipal water utilities, wastewater treatment plants, and regional distribution networks; many facilities rely on ICS and SCADA technologies. Increased intrusions in the water and wastewater sector highlight a broader strategy to gain persistent access to systems that would be strategically significant during a geopolitical conflict.

Tactics, Techniques, and Procedures

The water sector is particularly vulnerable to cyber threats. Many facilities, especially smaller utilities, rely on outdated technology. This is largely due to limited funding and technical staff. Poor patch management and misconfigured controls can exacerbate the problem, exposing critical systems on the web. Access typically begins with threat actors identifying vulnerable systems and leveraging known exploits to gain entry.

Third-party vendors are another common point of access. Water utilities often outsource services for IT support, SCADA system integration, remote monitoring, and more. These vendors are usually provided with privileged access to the control environments they service. By compromising a trusted partner, threat actors may be able to bypass system defenses and even gain administrative access to sensitive utility networks.

Threat actors utilize LoTL techniques once inside, leveraging legitimate credentials and native tooling to avoid triggering conventional alerts. They have been observed conducting internal reconnaissance to identify lateral movement paths across interconnected assets, including unmanaged OT endpoints and exposed admin shares. In cases where centralized logging was absent or poorly configured, they maintained persistence for extended periods without detection.

Credential theft is a core component of these operations. Threat actors may use tools such as Mimikatz to extract administrator and service account credentials from memory, which are then used to access additional systems or devices, including those that manage chemical dosing, pressure systems, or water flow rates. Critically, the IT and OT networks in water utilities are usually poorly segmented. This allows threat actors to move from administrative systems into operational environments using compromised accounts, where they can manipulate physical processes.

In targeted cases, threat actors may deploy custom malware. Variants of ShadowPad and China Chopper have been observed in such operations. This malware can be embedded within vendor support tools or disguised as legitimate software updates.

Recent and Notable Activity

China-linked threat actors have increasingly targeted the water and wastewater sector, exploiting poorly segmented OT networks and remote access tools maintained by third-party vendors. These intrusions have shifted from opportunistic probes to deliberate campaigns focused on gaining access to operational technology (OT) responsible for water treatment, chemical dosing, and distribution controls.

Chinese APT groups, including Volt Typhoon, have been observed targeting these facilities through unsecured remote access points and vendor software vulnerabilities. In several observed cases, attackers leveraged exposed VPN endpoints or compromised contractor accounts to access control systems running on legacy Windows servers and outdated SCADA interfaces. Once inside, they employ credential harvesting and living-off-the-land techniques to blend into legitimate administrative activity. Their access allows for the manipulation of physical processes and the disruption of water safety and availability—posing a direct threat to public health and civil stability in a conflict scenario.

In 2021, attackers attempted to manipulate chemical dosing levels at the Oldsmar, Florida, treatment facility via a remote access platform. More recently, in 2023, US officials warned of Chinese reconnaissance targeting utilities in Texas and Pennsylvania, using exposed VPNs and contractor credentials to access SCADA systems. These intrusions show a growing intent to manipulate physical processes and degrade civilian infrastructure readiness.

Implications and Impact

Many municipal water utilities operate with limited budgets and outdated infrastructure. As one of the most under-resourced domains, they often lack adequate means to implement cybersecurity measures. A large-scale cyberattack against the US water and wastewater sector would have grave implications for the health and well-being of communities nationwide. Threat actors can exploit critical security gaps to gain control over chemical dosing systems and water flow controllers. The impact would ripple through other industries, potentially disrupting the entire critical infrastructure system.

Almost immediately, the availability and safety of drinking water would be threatened. Disruptions at water treatment facilities could lead to service outages affecting thousands. In more severe attacks, treatment processes that manage and maintain safe chlorine or fluoride levels could be manipulated or used to introduce biological or chemical hazards.

National security and emergency response would also be impacted. Many military bases and defense contractors rely on civilian water systems. By disabling water services at or near

key facilities, cyberattacks could impair base operations and defense efforts. In addition, compromised water infrastructure could prevent emergency relief activities like firefighting and water purification during a crisis.

The economic consequences could be costly. Water services are foundational to various industries and municipal functions, and the financial costs of restoring service and mitigating contamination events would be substantial, especially for underfunded utilities that lack cyber insurance. Industries depending on clean water, including agriculture, manufacturing, and food processing, would face expensive shutdowns and product loss. Municipalities and local governments would bear significant financial burdens, from emergency infrastructure repairs to public communication efforts and potential legal liabilities.

Cyberattacks on the water sector also endanger public health and safety, as water could be polluted or become unavailable entirely. Hygiene and sanitation would quickly deteriorate, especially in densely populated areas. However, the impact could last beyond the immediate disruption to daily life. Contamination fears or service interruptions could fuel civil unrest and mistrust that lingers long after clean water access is restored.

Risk Assessment

The NJCCIC has assessed the water and wastewater sector as a critical risk due to its growing exposure to cyber intrusions and its essential role in public health and sanitation, infrastructure continuity, and military readiness. Both the likelihood and potential impact of a successful cyberattack are considered high. This assessment is based on the increased exposure of municipal and regional water utilities to industrial control system (ICS) compromise, particularly in facilities that rely on outdated technology. Chinese state-sponsored threat actors have demonstrated an interest in manipulating chemical dosing operations and disrupting water flow, which could threaten civilian safety and degrade operations across dependent sectors.

Transportation

Overview

The transportation sector is among the most interconnected elements of US infrastructure. It plays a vital role in commuting and travel, fuel distribution and supply chain networks, and military movement. China-linked APT groups likely view this domain as a tool of strategic disruption that can be exploited to impede national response capabilities. Transportation infrastructure includes rail signaling, port operations, fleet logistics systems, air traffic

control, and satellite-based navigation. Cyber activity against the sector often prioritizes persistent access and reconnaissance that threat actors can leverage during a geopolitical crisis.

Tactics, Techniques, and Procedures

The transportation sector is a broad network of distributed infrastructure that is facing increased exposure to cyberattacks. This includes customer portals, remote access platforms, SCADA systems, and more. One of the most frequent entry points are web-facing devices with known vulnerabilities. Many of these systems, particularly those from vendors like Fortinet and Pulse Secure, are targeted within hours of new exploits becoming publicly available.

Threat actors also target third-party vendors to infiltrate key networks. Many organizations in the transportation sector rely on external IT support, logistics software, maintenance contractors, and more. Service providers are often granted privileged system access, which threat actors can leverage to move laterally into the primary network.

Upon gaining access, the threat actors use LoTL techniques to evade detection. They abuse legitimate system tools to extract sensitive data and establish footholds. This approach helps them disguise their activity within legitimate traffic and maintain prolonged access across both IT and OT environments. It also minimizes the efficacy of detection software as they conduct reconnaissance and compromise additional systems on the network.

Credential theft is a common element of these attacks. Threat actors typically either dump LSASS memory or use tools like Mimikatz to extract valid account credentials. Weak segmentation between the It and OT environments is common in the transportation sector. This information can be used to escalate privileges and pivot across systems, transitioning into sensitive control domains.

Custom malware and backdoors may also be deployed. Variants like ShadowPad, PlugX, or China Chopper enable threat actors to maintain persistence or facilitate command-and-control. These tools are designed to blend in with regular network activity and avoid detection by endpoint security solutions.

Recent and Notable Activity

Chinese cyber activity against the transportation sector has expanded significantly, and APT groups are increasingly focused on transportation networks as critical chokepoints for supply chain disruption and military mobilization delay. Volt Typhoon and associated actors

have targeted operational systems in ports, rail control environments, and fleet management infrastructure. These campaigns often begin with the exploitation of VPN appliances, third-party logistics platforms, or exposed remote access interfaces. Threat actors then establish persistence and conduct reconnaissance to map dependencies and identify high-impact targets. Their objective is to pre-position within transportation networks and, if activated, disable or degrade transit operations at scale.

In 2023, Volt Typhoon was observed accessing rail signaling and port operations in Guam as part of a broader campaign targeting US Pacific infrastructure. CISA and TSA have also issued advisories regarding threats to transportation operators through VPN exploitation, third-party logistics platforms, and fleet management systems. These efforts suggest a deliberate strategy to map and impair operational systems at scale.

Implications and Impact

The transportation sector is an attractive target for adversaries seeking to disrupt the movement of people and goods. It includes road, rail, air, and maritime systems and the digital infrastructure used to coordinate fleet movements, cargo handling, and logistics. A well-timed intrusion could delay critical deliveries, stall flights or trains, and interfere with emergency mobilization, introducing risks to economic stability, national readiness, and public safety.

Civilian mobility would immediately falter, shutting down public transit systems and airways and stranding millions of people. Commercial logistics may also be impacted. Supply chain disruptions delaying the delivery of crucial goods could contribute to food and energy shortages that threaten national resiliency.

The US military would also be affected. Many defense logistics operations rely on civilian infrastructure for transportation. A cyberattack targeting key transportation networks could significantly disrupt national defense efforts. Critically, the mobilization of military equipment and personnel would be delayed, hindering the ability to organize forces and respond to a geopolitical crisis.

Risk Assessment

The NJCCIC has assessed the transportation sector as a critical risk due to its dependence on integrated IT and operational technology (OT) systems and its pivotal role in enabling national logistics, supply chain continuity, and disaster response. Both the likelihood and potential impact of a successful cyberattack are considered high. This assessment is based on mounting evidence of adversary reconnaissance and pre-positioning activity targeting

transportation networks and demonstrated capabilities to impair air traffic systems, rail signaling, maritime operations, and logistics platforms. Chinese state-sponsored actors have shown increasing interest in compromising operational control environments that support fleet management, port automation, and transit scheduling systems. These operations directly threaten troop deployment timelines, fuel and materiel distribution, and civilian mobility during a crisis. The sector's wide use of legacy OT systems, vendor-managed infrastructure, and often unmonitored remote access pathways further increases its exposure to targeted disruption.

Recommendations and Technical Guidance

Cybersecurity policies across all levels of operation are crucial for securing US critical infrastructure, particularly in the communications, energy, water and wastewater, and transportation sectors. Cyber activity sponsored by China will continue to target these high-risk sectors, threatening public safety and national security. To mitigate these risks, the NJCCIC advises that organizations implement layered defense strategies that prioritize strong cyber hygiene, detection and monitoring, and secure system architecture.

Resilient cybersecurity plans emphasize the importance of cyber hygiene, which encompasses the foundational practices that reduce exposure to common threats and prevent adversaries from gaining footholds within critical systems. Password reuse, weak credentials, and unsecured access points are among the top causes of system breaches. Employees should be required to create unique and complex passwords, and organizations should also enforce the use of password managers to avoid password reuse or other unsafe habits that increase the likelihood of account compromise. Multi-factor authentication (MFA) should be mandatory where available, especially for remote access, privileged accounts, and administrative interfaces. MFA adds a critical second layer of defense and ensures that unauthorized account access will be prohibited even if a password is compromised.

Additional cornerstones of cyber hygiene are effective patch management and secure system architecture. Cyberattacks against these sectors typically exploit known vulnerabilities for which patches already exist. Failing to apply software updates leaves systems exposed and vulnerable to threat activity. Organizations are advised to inventory all network assets, regularly track new vulnerabilities as they are disclosed, monitor for new patches as they become available, and prioritize addressing high-severity vulnerabilities immediately, especially those in web-facing or critical systems. Organizations should also implement network segmentation and intrusion detection. Backup procedures to ensure continuity during a ransomware attack or sabotage are recommended.

Each sector also presents unique risks and distinct operational challenges that organizations must address with tailored mitigations. These are outlined below.

Communications

To defend against APT groups like Volt Typhoon, organizations in the communications sector must implement hardened controls across both IT and OT systems, particularly where legacy telecom equipment intersects with modern IP-based routing and authentication services.

- Access to signaling infrastructure—including BGP routers, SS7 nodes, VoIP control systems, and DNS authoritative servers—should be strictly segmented and protected using multi-factor authentication (MFA) and role-based access controls (RBAC).

- Authentication services such as RADIUS, LDAP, and Kerberos ticketing systems should be continuously monitored for credential abuse, lateral movement, or the presence of tools like Mimikatz, which Volt Typhoon actors frequently use to dump credentials and tokens.

- Deploy network flow analysis (NetFlow/sFlow/IPFIX) and deep packet inspection (DPI) at internal chokepoints to identify anomalous routing updates, protocol abuse (e.g., unauthorized BGP route advertisements or malformed SS7 messages), or covert beaconing activity often used for command-and-control (C2).

- Ensure strict separation of management and operational planes in OT-adjacent telecom hardware, such as core switches, softswitches, and signaling gateways. This includes isolating control systems used for provisioning (e.g., SIP registrars or HLR/VLR databases) from external interfaces accessible via VPN or vendor support tunnels.

- Continuously validate the integrity of firmware and configuration baselines on edge devices such as firewalls, session border controllers (SBCs), and customer premises equipment (CPE), all of which have been targeted in Volt Typhoon's low-profile, living-off-the-land campaigns.

Energy

Chinese APTs such as APT41 and Volt Typhoon have demonstrated the capability to persist within ICS/SCADA environments, often by pivoting from exposed IT assets into OT domains. Energy providers must focus on strict IT/OT segmentation, credential hygiene, and visibility within industrial control protocols.

- DMZ architecture must enforce unidirectional data flow between corporate IT and control systems (e.g., historian push-only to IT). Access to HMI terminals, PLC programming interfaces, and SCADA servers must be isolated from remote administration portals unless tunneled through secure jump servers with full session recording.

- Monitor for lateral movement tools such as Impacket, PsExec, and remote WMI—all frequently used by Volt Typhoon to traverse ICS-connected Windows environments. Alert on unauthorized use of SMB, RDP, and RPC across OT VLANs.

- Deploy deep packet inspection for ICS protocols like Modbus, DNP3, OPC, and IEC 60870-5-104. Look for out-of-sequence function codes, changes to control points, or rogue devices issuing write commands—a strong indicator of adversary presence.

- Use asset inventory and passive OT monitoring tools (e.g., Nozomi, Claroty, Dragos) to baseline expected communications and detect anomalous command traffic or firmware changes on field devices.

- APT41 has previously weaponized vendor support tools and outdated VPN concentrators to establish long-term access. All vendor access should be time-bound, approval-based, and recorded, with telemetry exported to a centralized SIEM for correlation with ICS activity.

Water and Wastewater

Water utilities—especially smaller or municipal ones—are frequent targets due to outdated ICS, limited logging, and reliance on third-party vendors. Volt Typhoon and other Chinese actors aim to manipulate chemical dosing, pump control, or SCADA telemetry to degrade water quality or disable distribution.

- All remote access to water SCADA systems (chlorine dosing, booster stations, flow control) must go through hardened gateways with multi-factor authentication, geofencing, and IP allowlisting.

- Monitor authentication logs for repeated failed logins or anomalous logon times, especially on Windows-based HMI systems. Volt Typhoon actors often perform after-hours access and escalate privileges via token impersonation or LSASS dumping.

- Segment treatment plant operational systems from billing/customer portals and vendor maintenance workstations. Firewalls should strictly block inbound access to OT devices unless traffic originates from safelisted jump boxes.

- Use change detection tools to monitor for alterations in PLC ladder logic, setpoint values, or firmware revisions—especially in devices managing chemical injectors or pump pressure.

- Establish baselines for regular ICS command traffic and SCADA polling intervals. Anomalies in polling frequency, device command latency, or unsolicited write requests can indicate adversarial manipulation.

Transportation

Transportation infrastructure—including rail systems, air traffic control, port operations, and fleet logistics platforms—faces growing risk from Chinese threat actors who aim to delay military mobilization and disrupt supply chains during geopolitical escalation.

- Ensure SCADA and logistics control networks (e.g., rail signaling, airport runway systems, port crane automation) are physically and logically segmented from public-facing systems such as passenger portals or scheduling apps.

- Deploy protocol-aware intrusion detection systems (IDS) for transport-related OT, such as CAN bus, Profinet, and serial-over-IP traffic used in legacy rail and aviation systems. Volt Typhoon has used stealthy C2 over nonstandard ports to evade detection in these environments.

- Monitor for abuse of transportation vendor APIs (e.g., automated shipping manifests, flight route uploads), which can be manipulated to disrupt service continuity or spoof departure/arrival data.

- Secure backend databases for fleet management, geolocation tracking, and fuel logistics with strong role-based access controls. Prior incidents have shown that weak permissions on logistics systems allow lateral movement into control environments.

- Audit all remote connections—especially unmanaged cellular modems, satellite uplinks, and VPN appliances used in mobile transportation contexts—and deploy EDR agents on endpoints used for remote dispatch or route programming.

Sustained security across these sectors depends on integrating cybersecurity into daily operations. Cybersecurity plans must outline and enforce basic cyber best practices to reduce risk exposure and improve the ability of critical infrastructure organizations to respond to emerging threats. Regular risk assessments can further assist organizations in identifying potential vulnerabilities and evaluating the likelihood and severity of risks.

Conclusion

Chinese state-sponsored threat activity constitutes a critical risk to US national security, economic stability, and public safety. As detailed in this report, APT groups such as Volt Typhoon, APT41, and Salt Typhoon are actively engaged in campaigns designed to infiltrate and establish persistent access within key tiers of US critical infrastructure. These operations are strategic, intending to enable widespread disruption during a future conflict, particularly involving heightened tensions in the Indo-Pacific region and Taiwan.

The communications, energy, water and wastewater, and transportation sectors are at the highest level of risk. These sectors provide fundamental services, directly supporting emergency response, military readiness, supply chain continuity, and the daily functioning of civilian life. The NJCCIC's risk assessment highlights the probability of continued cyber activity and the consequences of successful intrusions, which range from mass service outages and economic losses to degraded defense capabilities and compromised public health and well-being.

Tactics employed by Chinese-sponsored APT groups highlight a deliberate effort to pre-position for maximum operational disruption. These include the exploitation of unpatched vulnerabilities, credential theft, lateral movement across poorly segmented networks, and deploying stealthy backdoors within IT and operational technology environments. Leveraging legitimate access methods and living-off-the-land techniques further enables long-term persistence and evasion of traditional detection methods. Given the significance of target sectors, organizations are advised to implement proactive defense measures to counter these threats.

Cyber operations are expected to continue as China-linked actors expand their campaigns to degrade or disable essential US critical infrastructure from within. Countering these threats will require sustained coordination among organizations across the

communications, energy, water and wastewater, and transportation sectors in collaboration with state and local governments, federal agencies, and private-sector stakeholders. The NJCCIC will continue to monitor developments related to this cyber activity. As new information becomes available, ongoing analysis and threat intelligence updates will be provided.

Sources

Microsoft. (2023, May 24). Volt Typhoon: State-aligned actor gaining access to critical infrastructure in the U.S..

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), & Department of Energy (DOE). (2023, May 24). People's Republic of China state-sponsored cyber actor living off the land to evade detection.

Cybersecurity and Infrastructure Security Agency (CISA). (2023, December). Top cyber actions for securing water systems.

Mandiant. (2020, March 25). APT41: A dual espionage and cyber crime operation.

Recorded Future. (2021, March 10). RedEcho targets Indian critical infrastructure with ShadowPad backdoor.

Dragos. (2022). CHERNOVITE and PIPEDREAM: Threat activity targeting industrial control systems.

The New York Times. (2023, July 28). Chinese hacking of U.S. infrastructure raises alarms.

CNN. (2023, July 28). Chinese hackers breach U.S. infrastructure, raise fears of sabotage.

Cybersecurity and Infrastructure Security Agency (CISA). (2021, May 11). DarkSide ransomware impacting Colonial Pipeline.

Miller, C. (2022, September 15). TSMC and the geopolitics of chipmaking: How Taiwan became the center of the world. Time.

Time. (2022, September 28). Why protecting Taiwan really matters to the U.S..

The Cipher Brief. (2023, July 31). Top U.S. cybersecurity official: China attacks on American infrastructure 'tip of the iceberg'.

Industrial Cyber. (2024, March 13). U.S. House Committee warns of homeland security threats from CCP hackers and transnational criminals, urging action.

MITRE ATT&CK. (n.d.). APT41.

MITRE ATT&CK. (n.d.). Volt Typhoon.