Foreign Technology Threats in Government Electronics: A 2009-2024 Review

Report Date: 2025-09-17

Executive Summary

This report provides a comprehensive analysis of foreign technology threats, including malware, hardware trojans, and counterfeit components, discovered in imported electronics used by government entities in the United States from 2009 to 2024. The increasing reliance on globalized supply chains has created significant vulnerabilities, which have been systematically exploited by nation-state actors and sophisticated criminal organizations. This document chronicles documented cases where such threats were identified, organizing findings by threat category and chronologically to illustrate the evolving nature of these security challenges. The primary threat actors identified are affiliated with China, Russia, Iran, and North Korea, each employing distinct tactics to achieve objectives ranging from espionage and intellectual property theft to disruption of critical infrastructure. The findings underscore the urgent need for robust supply chain risk management, enhanced procurement protocols, and proactive cybersecurity defenses across all levels of government—federal, state, county, and city.

Hardware Trojans and Supply Chain Compromises

Hardware trojans represent one of the most insidious threats to government electronics, involving malicious modifications to integrated circuits or other components during the manufacturing process. These compromises are difficult to detect and can provide adversaries with persistent, low-level access to sensitive systems. The global electronics supply chain, with its heavy reliance on overseas manufacturing, particularly in China, presents a prime environment for such attacks. Government procurement processes, often prioritizing cost-efficiency, can inadvertently introduce these compromised components into critical infrastructure, defense systems, and administrative networks. The following documented cases highlight the persistent risk of hardware-level backdoors in imported technology.

The Big Hack: China's Microchip Infiltration

- **Title:** The Big Hack: How China Used a Tiny Chip to Infiltrate America's Top Companies
- **Publication Date:** October 4, 2018
- **Source:** Bloomberg
- **Direct Link:** https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

- **Summary:** This investigative report details a 2015 incident where Chinese intelligence operatives allegedly compromised the U.S. technology supply chain by embedding a tiny microchip onto server motherboards manufactured by Supermicro. These compromised motherboards were used by major U.S. companies, including Amazon and Apple, and were also supplied to government agencies, including the Department of Defense and CIA. The malicious chip was designed to create a stealth backdoor, allowing attackers to access sensitive corporate and government data. The attack highlighted the profound vulnerabilities inherent in outsourcing the manufacturing of critical electronic components.

Safeguarding the Military's Cyber Supply Chain

- **Title:** Safeguarding the United States Military's Cyber Supply Chain
- **Publication Date:** Not specified (inferred context post-2017)
- **Source:** Cyber Defense Review (army.mil)
- **Direct Link:** https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136092/safeguarding-the-united-states-militarys-cyber-supply-chain/
- **Summary:** This analysis discusses the significant risks posed to the U.S. military by its reliance on Chinese firms for technology and manufacturing. It highlights vulnerabilities created by outsourcing, which can lead to the insertion of backdoors in critical equipment and the introduction of counterfeit parts into the defense supply chain. The article points to specific concerns, such as compromised components in U.S. aircraft and potential backdoors in port equipment, underscoring the national security threat. It calls for a strategic balance between economic engagement with China and the implementation of stringent security measures to protect military assets.

Chinese Espionage Threats to U.S. Ports

- **Title:** What They Are Saying: Joint Investigation Finds Potential Chinese Espionage Threats to U.S. Ports
- **Publication Date:** September 16, 2024
- **Source:** House Committee on Homeland Security
- **Direct Link:** https://homeland.house.gov/2024/09/16/what-they-are-saying-joint-investigation-finds-potential-chinese-espionage-threats-to-u-s-ports/
- **Summary:** A joint congressional investigation revealed significant security threats posed by Chinese-manufactured cranes used in U.S. ports, many of which serve military functions. The report found that equipment from state-owned enterprise Shanghai Zhenhua Heavy Industries (ZPMC) could contain backdoors or communications devices that enable espionage and disruption. These vulnerabilities could allow China to remotely access sensitive logistics data or even manipulate port operations during a conflict.

The findings prompted calls for greater scrutiny of foreign-made equipment procured for critical infrastructure.

Federal Agency Failures in Supply Chain Risk Management

- **Title:** INFORMATION AND COMMUNICATIONS TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks
- **Publication Date:** December 16, 2020
- **Source:** U.S. Government Accountability Office (GAO)
- **Direct Link:** https://www.gao.gov/assets/gao-21-171.pdf
- **Summary:** This GAO report assessed 23 federal agencies and found that very few had implemented foundational practices for managing information and communications technology (ICT) supply chain risks. The report highlights that agencies are vulnerable to threats from counterfeit components and malicious code inserted by foreign adversaries during manufacturing. The widespread failure to establish supplier reviews, conduct risk assessments, or implement processes for detecting compromised products leaves government procurement channels dangerously exposed to backdoor trojans and other hardware-based attacks.

State-Sponsored Malware Campaigns (APT Groups)

Nation-state actors, operating through Advanced Persistent Threat (APT) groups, conduct sophisticated and sustained malware campaigns against government entities. These operations are designed for espionage, data theft, and pre-positioning for future disruptive attacks on critical infrastructure. Using custom malware, zero-day exploits, and stealthy "living-off-the-land" techniques, these groups infiltrate federal, state, and local government networks, often remaining undetected for extended periods. The following sections detail campaigns attributed to actors from China, Russia, Iran, and North Korea.

Chinese State-Sponsored Actors

China operates a vast and highly capable cyber apparatus that targets government and critical infrastructure sectors globally. Groups such as Volt Typhoon and Salt Typhoon specialize in stealthy infiltration, using compromised network devices and legitimate system tools to evade detection while gaining access to sensitive networks.

- **Title:** Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques
- **Publication Date:** May 24, 2023
- **Source:** Microsoft Security Blog

- **Direct Link:** https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
- **Summary:** Microsoft identified a Chinese state-sponsored actor, Volt Typhoon, engaged in a campaign targeting U.S. critical infrastructure, including in Guam. Active since mid-2021, the group focuses on espionage and pre-positioning for future disruptive attacks by using "living-off-the-land" techniques, which involve using built-in network administration tools to blend in with normal activity. This stealthy approach allows the group to maintain long-term persistence while compromising communications, energy, transportation, and government sectors. The campaign's focus on strategic locations suggests an intent to disrupt critical communications between the U.S. and the Asia region during future crises.
- **Title:** U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure
- **Publication Date:** January 31, 2024
- **Source:** U.S. Department of Justice
- **Direct Link:** https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
- **Summary:** The U.S. Department of Justice announced a court-authorized operation to disrupt a botnet controlled by the Chinese state-sponsored group Volt Typhoon. The botnet consisted of hundreds of compromised small office/home office (SOHO) routers, which the hackers used as a proxy network to conceal their malicious activities against U.S. critical infrastructure. This action aimed to sever the connection between the compromised devices and the attackers, but officials warned that the threat actor remains active. The operation highlights the use of common, insecure consumer-grade electronics to facilitate attacks on high-value government and infrastructure targets.
- **Title:** Salt Typhoon hackers targeted over 80 countries, FBI says
- **Publication Date:** August 20, 2025
- **Source:** Nextgov
- **Direct Link:** https://www.nextgov.com/cybersecurity/2025/08/salt-typhoon-hackers-targeted-over-80-countries-fbi-says/407719/
- **Summary:** The FBI revealed that the Chinese state-sponsored hacking group Salt Typhoon compromised telecommunications companies and government entities in over 80 countries as part of a massive espionage campaign. The group exploited vulnerabilities in network devices to gain access to call detail records and other sensitive metadata, targeting high-profile individuals, including U.S. government officials. This widespread

breach, considered one of the worst in U.S. history, compromised critical infrastructure sectors and posed a significant threat to national security. The campaign demonstrates China's capability to conduct large-scale, long-term intelligence gathering operations via telecommunications networks.

Russian State-Sponsored Actors

Russian intelligence services, including the FSB, SVR, and GRU, direct some of the world's most aggressive and disruptive cyber operations. These actors have targeted government systems with destructive malware, conducted large-scale supply chain attacks, and sought to compromise critical infrastructure. Groups like APT29 (Cozy Bear) and Sandworm are known for their sophisticated tactics and their alignment with Russia's geopolitical objectives.

- **Title:** Russian Government Cyber Actors Targeting Network Devices
- **Publication Date:** August 20, 2025
- **Source:** FBI Internet Crime Complaint Center (IC3)
- **Direct Link:** https://www.ic3.gov/PSA/2025/PSA250820
- **Summary:** The FBI issued a Private Sector Advisory warning that Russian state-sponsored cyber actors were targeting networking devices and associated infrastructure globally. The advisory details how these actors exploit vulnerabilities in routers and other network equipment to conduct espionage, steal intellectual property, and disrupt networks. This campaign affects a wide range of sectors, including government agencies, and serves as a reminder of the persistent threat posed by Russian intelligence services to critical U.S. systems.
- **Title:** Russian SVR Targets U.S. and Allied Networks
- **Publication Date:** April 20, 2022
- **Source:** Cybersecurity and Infrastructure Security Agency (CISA)
- **Direct Link:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
- **Summary:** This joint advisory from CISA and allied agencies details the tactics, techniques, and procedures (TTPs) used by the Russian Foreign Intelligence Service (SVR), also known as APT29 or Cozy Bear. The group is responsible for the SolarWinds supply chain attack, which compromised numerous U.S. federal agencies and private sector organizations. The advisory notes that APT29 continues to target government, technology, and energy sectors, using sophisticated malware and exploiting cloud services to maintain persistent access and exfiltrate sensitive information.
- **Title:** Three states were compromised in SolarWinds hack, CISA official says

- **Publication Date:** February 26, 2021
- **Source:** StateScoop
- **Direct Link:** https://statescoop.com/cozybear-solarwinds-three-states/
- **Summary:** A CISA official confirmed that at least three U.S. state governments were compromised as part of the massive SolarWinds supply chain attack attributed to the Russian-backed group APT29. The attackers inserted a backdoor into the SolarWinds Orion software, which was then distributed to thousands of government and corporate customers. This allowed the hackers to gain access to state government networks, posing a significant risk of data theft and further system compromise. The incident highlighted the vulnerability of state and local governments to sophisticated, nation-state supply chain attacks.
- **Title:** Understanding Sandworm, a State-Sponsored Threat Group
- **Publication Date:** 2024
- **Source:** ISACA
- **Direct Link:** https://www.isaca.org/resources/news-and-trends/industry-news/2024/understanding-sandworm-a-state-sponsored-threat-group
- **Summary:** This article provides an overview of Sandworm, a threat group linked to Russia's GRU military intelligence agency, known for its destructive cyberattacks. Sandworm was responsible for the 2015 and 2016 power grid outages in Ukraine using the Industroyer malware and the global NotPetya wiper attack in 2017, which caused billions in damages. The group's activities demonstrate a clear intent to disrupt and destroy critical infrastructure, including government systems, as part of Russia's hybrid warfare strategy.

Iranian and North Korean State-Sponsored Actors

APT groups from Iran and North Korea are increasingly sophisticated, targeting government networks for espionage, financial gain, and disruption. North Korean groups, such as the Lazarus Group, are notorious for financially motivated attacks, including ransomware campaigns and cryptocurrency theft, to fund the regime. Iranian actors, often linked to the IRGC, focus on intelligence gathering and retaliatory attacks against regional and Western adversaries.

- **Title:** Andariel, a North Korean APT Group, Targets Military and Nuclear Programs
- **Publication Date:** Not specified (inferred 2024 context)
- **Source:** Picus Security
- **Direct Link:** https://www.picussecurity.com/resource/blog/andariel-north-korean-apt-group-targets-military-and-nuclear-programs

- **Summary:** The North Korean APT group Andariel, a subgroup of the Lazarus Group, has been actively targeting military, nuclear, and defense entities for cyber espionage and financial gain. The group exploits public-facing applications and uses custom malware and ransomware to infiltrate government networks in South Korea and the United States. Their operations focus on stealing sensitive military intelligence and generating revenue for the North Korean regime through activities like ATM hacking and bank card theft.
- **Title:** State-Aligned APT Groups Increasingly Deploying Ransomware
- **Publication Date:** November 2, 2022
- **Source:** WeLiveSecurity by ESET
- **Direct Link:** https://www.welivesecurity.com/en/business-security/state-aligned-apt-groups-increasingly-deploying-ransomware/
- **Summary:** This report observes a growing trend of state-aligned APT groups from Iran, North Korea, and China using ransomware in their attacks. While some attacks are financially motivated, others use ransomware as a decoy to disguise espionage operations or as a destructive tool to wipe data. The analysis highlights groups like Iran's Pioneer Kitten, which collaborates with ransomware affiliates to target government and critical infrastructure entities in the U.S. and the Middle East.
- **Title:** Iranian Cyber Attacks in 2025: What to Expect
- **Publication Date:** 2025
- **Source:** Palo Alto Networks Unit 42
- **Direct Link:** https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/
- **Summary:** This threat assessment from Unit 42 outlines the evolving capabilities of Iranian APT groups, such as APT42, which is affiliated with the IRGC. These groups employ spear-phishing, social engineering, and malware to target government, military, and defense sectors, particularly in the U.S. and the Middle East. The report notes an increase in destructive wiper malware and the use of generative AI to enhance social engineering campaigns, indicating a growing sophistication in Iran's state-sponsored cyber operations.

Counterfeit Electronics

The infiltration of counterfeit electronic components into government supply chains poses a severe threat to national security, public safety, and mission readiness. These parts, often sourced from China, are misrepresented as genuine and can range from remarked used components to poorly manufactured copies.

Their inclusion in critical systems, such as military hardware and infrastructure controls, can lead to catastrophic failures, create hidden vulnerabilities for exploitation, and undermine the integrity of U.S. defense and government systems.

- **Title:** Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts
- **Publication Date:** May 21, 2012
- **Source:** U.S. Senate Committee on Armed Services
- **Direct Link:** https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts
- **Summary:** A year-long investigation by the Senate Armed Services Committee uncovered over one million suspected counterfeit electronic parts in the Department of Defense supply chain. The report traced a majority of these components to China and found them in critical military systems, including thermal weapons sights, missile guidance systems, and military aircraft. The investigation concluded that this flood of counterfeit parts poses a significant risk to national security and the safety of U.S. military personnel.
- **Title:** Federal Agencies Launch 'Operation Chain Reaction' to Protect Critical Supply Chains
- **Publication Date:** July 12, 2012
- **Source:** U.S. Immigration and Customs Enforcement (ICE)
- **Direct Link:** https://www.ice.gov/news/releases/federal-agencies-launch-operation-chain-reaction
- **Summary:** In response to the growing threat, federal agencies including ICE, CBP, and the FBI launched "Operation Chain Reaction." This initiative was designed to target the trafficking of counterfeit integrated circuits and other electronic components entering the supply chains of the Department of Defense and other U.S. government agencies. The operation aimed to protect national security, public safety, and the warfighter by disrupting criminal networks that profit from selling fake and substandard parts.
- **Title:** Senate bill would ban agency purchases of counterfeit electronics
- **Publication Date:** March 1, 2023
- **Source:** FedScoop
- **Direct Link:** https://fedscoop.com/senate-bill-would-ban-agency-purchases-of-counterfeit-electronics/

- **Summary:** A bipartisan bill, the Securing America's Federal Equipment (SAFE) in Supply Chains Act, was introduced in the Senate to combat the threat of counterfeit electronics. The legislation would prohibit federal agencies from purchasing electronic products and components from unauthorized sellers. This measure aims to enhance cybersecurity and supply chain integrity by ensuring that government procurement relies on trusted and vetted distributors, thereby reducing the risk of acquiring compromised or substandard parts.

Signal Jammers and Physical Hardware Threats

Beyond digital infiltration, foreign threats also manifest through physical hardware designed to disrupt government operations. The smuggling of devices like signal jammers, primarily manufactured in China, poses a direct threat to law enforcement, emergency services, and correctional facilities. These devices can disable critical communications, GPS, and drone operations, enabling criminal activity and undermining public safety and security protocols within government-managed environments.

- **Title:** Homeland Security Warns About Spike in China-Based Technology Firms Smuggling Signal Jammers
- **Publication Date:** June 18, 2025
- **Source:** U.S. Department of Homeland Security (DHS)
- **Direct Link:** https://www.dhs.gov/news/2025/06/18/homeland-security-warns-about-spike-china-based-technology-firms-smuggling-signal
- **Summary:** The DHS issued a warning about a significant increase in the smuggling of signal jammers manufactured by Chinese firms into the United States, with seizures rising 830% since 2021. These illegal devices are used by criminals, including illegal aliens, to disrupt law enforcement communications, GPS tracking, and security systems during crimes like burglaries and bank robberies. The surge poses a direct threat to public safety and national security, with DHS labeling the devices as "tools of terrorism."
- **Title:** Illegal Chinese jammers used in Vermont bank robberies, DHS says
- **Publication Date:** Not specified (inferred 2025 context)
- **Source:** Vermont Daily Chronicle
- **Direct Link:** https://vermontdailychronicle.com/illegal-chinese-jammers-used-in-vermont-bank-robberies-dhs-says/
- **Summary:** This article reports on specific instances where Chinese-manufactured signal jammers were used in criminal activities affecting local government functions. According to the DHS, these devices were linked to bank robberies in Vermont, where they were used to disrupt

law enforcement and security communications. This case exemplifies how smuggled foreign technology directly enables crimes that challenge the operational capacity of local and state police forces.

- **Title:** Bureau of Prisons Tests Micro-Jamming Technology at South Carolina Prison to Prevent Contraband Cell Phone Use
- **Publication Date:** Not specified (inferred post-2018)
- **Source:** U.S. Department of Justice
- **Direct Link:** https://www.justice.gov/archives/opa/pr/bureau-prisons-tests-micro-jamming-technology-south-carolina-prison-prevent-contraband-cell
- **Summary:** The Federal Bureau of Prisons (BOP) conducted a test of micro-jamming technology at a federal prison to combat the use of contraband cell phones by inmates. While this case involves a government agency using jamming technology as a countermeasure, it highlights the underlying threat posed by unauthorized communications within secure government facilities. The need for such technology underscores the challenge of preventing inmates from coordinating criminal activities or communicating with outside contacts using smuggled devices.

Specific Imported Hardware in Government Facilities

This section documents specific cases where imported hardware components were actually deployed in federal, state, county, or city government facilities and later discovered to contain security vulnerabilities, backdoors, or malware. These incidents highlight the risks posed by foreign-manufactured hardware in sensitive government environments.

Battery Management Systems and Energy Storage

- **Title:** Duke Energy to phase out Chinese batteries due to hacking concerns
- **Publication Date:** December 2023
- **Source:** WRAL News
- **Direct Link:** https://www.wral.com/story/duke-energy-to-phase-out-chinese-batteries-due-to-hacking-concerns/21276994/
- **Summary:** Duke Energy installed CATL-manufactured batteries in a solar energy storage system at Marine Corps Base Camp Lejeune in North Carolina in March 2023, but security concerns arose regarding potential backdoors and unauthorized communication with Chinese entities. U.S. lawmakers pressured Duke Energy to decommission the system due to fears of exploitation by PRC state-sponsored actors like Volt Typhoon. By December 2023, Duke Energy disconnected and planned to phase out the CATL batteries, citing risks of malware insertion and data exfiltration. The incident highlighted how battery management systems could serve as

entry points for espionage or disruption of military operations and critical infrastructure.

CCTV and Surveillance Systems

- **Title:** Canada has ordered Hikvision Canada Inc. to cease operations
- **Publication Date:** 2025
- **Source:** Infosecurity Magazine
- **Direct Link:** https://www.infosecurity-magazine.com/news/canada-bans-chinese-cctv-hikvision/
- **Summary:** Following a national security review under the Investment Canada Act, Canada mandated that Hikvision Canada Inc. cease operations and prohibited federal institutions from purchasing or using its surveillance products. The ban extended to legacy equipment reviews and echoed similar actions by other governments concerned about cybersecurity risks and potential backdoors in Chinese-manufactured CCTV systems. UK government entities, including the Ministry of Defence and various local councils, have also removed or banned Hikvision cameras due to security and ethical concerns, with approximately 50% of sensitive sites updated by 2024. These actions stem from identified vulnerabilities such as a 2017 backdoor and a 2021 web attack vulnerability (CVE-2021-36260) that allows unauthenticated remote code execution.
- **Title:** Vulnerabilities Identified in Dahua Hero-C1 Smart Cameras
- **Publication Date:** 2025
- **Source:** Bitdefender
- **Direct Link:** https://www.bitdefender.com/en-us/blog/labs/vulnerabilities-identified-in-dahua-hero-c1-smart-cameras
- **Summary:** Bitdefender identified two critical vulnerabilities (CVE-2025-31700 and CVE-2025-31701) in Dahua cameras involving stack-based and segment buffer overflows that allow unauthenticated remote code execution. These flaws affect over 100 Dahua models, including popular series like IPC and SD, and could enable attackers to bypass firmware checks and deploy persistent malware that makes devices difficult to clean. The Vatican City had deployed Dahua cameras for security but faced concerns about data breaches, potential backdoors, and geopolitical implications due to the manufacturer's ties to Chinese entities. Historical vulnerabilities in Dahua cameras included a significant backdoor discovered in 2017 that allowed attackers to download user databases and gain control of devices, which was exploited to infect nearly one million devices with BASHLITE malware.

Network Equipment and Infrastructure

- **Title:** PRC State-Sponsored Cyber Actors Exploit Network Devices for Persistent Access
- **Publication Date:** August 2025
- **Source:** CISA
- **Direct Link:** https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
- **Summary:** CISA documented how PRC state-sponsored actors systematically exploited vulnerabilities in network devices, including routers and switches, to gain persistent access to government and critical infrastructure networks. The actors modified access control lists (ACLs), enabled non-standard ports for remote access, and used custom scripts to evade detection on devices from manufacturers like Cisco and Juniper. Specific incidents included backdooring Juniper MX routers with custom malware like TinyShell and exploiting Cisco IOS XE routers through vulnerabilities such as CVE-2023-20198 and CVE-2023-20273. These compromises affected government facilities by allowing adversaries to pivot into sensitive networks, exfiltrate data, and maintain long-term persistence for espionage and potential disruption.
- **Title:** U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure
- **Publication Date:** January 31, 2024
- **Source:** U.S. Department of Justice
- **Direct Link:** https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
- **Summary:** The DOJ announced a court-authorized operation to disrupt a botnet controlled by the Chinese state-sponsored group Volt Typhoon, consisting of hundreds of compromised small office/home office (SOHO) routers used as a proxy network. The botnet included compromised Cisco and NETGEAR devices that were used to conceal malicious activities against U.S. critical infrastructure, including government facilities. These consumer-grade routers, many of which were end-of-life devices lacking security updates, served as entry points for broader network infiltration and espionage operations. The operation highlighted how ubiquitous networking equipment, often imported and widely deployed in government facilities, can be weaponized by foreign adversaries to facilitate attacks on high-value targets.

Industrial Control Systems and SCADA

- **Title:** Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques
- **Publication Date:** May 24, 2023
- **Source:** Microsoft Security Blog
- **Direct Link:** https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
- **Summary:** Microsoft identified Chinese state-sponsored actors compromising industrial control systems (ICS) and SCADA systems in U.S. government facilities and critical infrastructure, including communications, energy, transportation, and water sectors. The Volt Typhoon group achieved lateral movement from IT networks to operational technology (OT) assets, potentially enabling disruption of systems like heating, ventilation, and air conditioning or water controls in government buildings. These actors tested access to OT assets with default credentials and extracted sensitive data like Active Directory databases (NTDS.dit files) to facilitate persistent access. The campaign's focus on strategic locations, including facilities in Guam, suggests an intent to disrupt critical communications and infrastructure during future crises, with government facilities serving as key targets for espionage and pre-positioning for destructive attacks.

Medical Devices and Healthcare Equipment

- **Title:** China-made medical devices are all over the U.S. and the feds are worried
- **Publication Date:** February 23, 2025
- **Source:** CNBC
- **Direct Link:** https://www.cnbc.com/2025/02/23/china-made-medical-devices-are-all-over-us-and-the-feds-are-worried.html
- **Summary:** The FDA and CISA issued warnings about Chinese-manufactured medical devices, specifically the Contec CMS8000 patient monitor, which contains exploitable backdoors that could alter configurations and compromise patient data. These devices are widely deployed in U.S. hospitals, including those serving government employees and military personnel, creating risks of remote exploitation that could lead to incorrect medical decisions or data breaches. While no known incidents have occurred, the vulnerability demonstrates the proliferation of insecure Chinese medical equipment in sensitive healthcare environments. This represents a broader pattern where cost-driven adoption of Chinese healthcare technology creates strategic risks, prompting federal agencies to work toward incentivizing domestic production and improving device security standards.

Energy Infrastructure Components

- **Title:** Ghost in the machine: Rogue communication devices found in Chinese inverters
- **Publication Date:** May 14, 2025
- **Source:** Reuters
- **Direct Link:** https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
- **Summary:** U.S. experts discovered undocumented cellular radios and communication devices in Chinese-manufactured solar inverters that could bypass firewalls and enable unauthorized remote access to energy systems. These rogue components were not listed in product documentation and posed security risks to critical infrastructure, including government facilities utilizing solar energy systems. The Department of Energy acknowledged these risks and stressed the need for better disclosure through tools like Software Bill of Materials (SBOMs) to address gaps in manufacturer transparency. The discovery highlighted broader concerns about Chinese energy infrastructure components potentially containing backdoors or communication channels that could be exploited for espionage or disruption of power systems serving government facilities.

Port and Maritime Infrastructure

- **Title:** New Investigation Finds Potential Chinese Threats to U.S. Port Infrastructure Security
- **Publication Date:** September 12, 2024
- **Source:** House Committee on Homeland Security
- **Direct Link:** https://homeland.house.gov/2024/09/12/new-investigation-by-house-homeland-select-committee-on-the-ccp-finds-potential-chinese-threats-to-u-s-port-infrastructure-security/
- **Summary:** A joint congressional investigation revealed that Chinese company Shanghai Zhenhua Heavy Industries (ZPMC) dominates the U.S. market for ship-to-shore cranes, with equipment installed at ports that serve military and government functions. Investigators found undocumented cellular modems on ZPMC cranes and evidence of the company requesting remote access capabilities, raising cybersecurity concerns about unauthorized data collection or system manipulation. These cranes are critical infrastructure components that handle sensitive military and government cargo, making them attractive targets for espionage or sabotage operations. The investigation highlighted how foreign-manufactured port equipment could provide persistent access points for intelligence gathering or potential disruption of supply chains vital to national security and government operations.

Local Government Software and Systems

- **Title:** US local governments targeted by Chinese hackers exploiting zero-day vulnerability
- **Publication Date:** 2025
- **Source:** SecurityWeek
- **Direct Link:** https://www.securityweek.com/cityworks-zero-day-exploited-by-chinese-hackers-in-us-local-government-attacks/
- **Summary:** Chinese threat actors exploited a zero-day vulnerability (CVE-2025-0994) in Trimble Cityworks software, a Geographic Information System used by county and city governments for managing infrastructure like utilities and public services. The attackers deployed malware including Rust-based loaders and Cobalt Strike beacons to gain persistent access and pivot to utilities management systems serving local government operations. Custom malware written in Chinese indicated state affiliation, with Cisco Talos tracking the campaign as targeting enterprise networks of local governing bodies. While primarily software-based, the attack affected hardware components like Microsoft IIS web servers and demonstrated how vulnerabilities in imported or foreign-influenced technology can compromise critical municipal infrastructure and government services.

References

The Big Hack: How China Used a Tiny Chip to Infiltrate America's Top Companies - Bloomberg Safeguarding the United States Military's Cyber Supply Chain - Cyber Defense Review What They Are Saying: Joint Investigation Finds Potential Chinese Espionage Threats to U.S. Ports - House Committee on Homeland Security INFORMATION AND COMMUNICATIONS TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks - U.S. Government Accountability Office Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques - Microsoft Security Blog U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure - U.S. Department of Justice Salt Typhoon hackers targeted over 80 countries, FBI says - Nextgov Russian Government Cyber Actors Targeting Network Devices - FBI IC3 Russian SVR Targets U.S. and Allied Networks - CISA Three states were compromised in SolarWinds hack, CISA official says - StateScoop Understanding Sandworm, a State-Sponsored Threat Group - ISACA Andariel, a North Korean APT Group, Targets Military and Nuclear Programs - Picus Security State-Aligned APT Groups Increasingly Deploying Ransomware - WeLiveSecurity Iranian Cyber Attacks in 2025: What to Expect - Palo Alto Networks Unit 42 Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts - U.S. Senate Committee on Armed Services Federal Agencies Launch 'Operation Chain Reaction' to Protect Critical Supply Chains - U.S. Immigration and Customs Enforcement Senate bill would ban agency purchases of counterfeit electronics - FedScoop Homeland Security Warns About Spike in China-Based Technology Firms Smuggling Signal

Jammers - U.S. Department of Homeland Security Illegal Chinese jammers used in Vermont bank robberies, DHS says - Vermont Daily Chronicle Bureau of Prisons Tests Micro-Jamming Technology at South Carolina Prison to Prevent Contraband Cell Phone Use - U.S. Department of Justice HC3 Threat Briefing: Chinese State-Sponsored Cyber Activity - AHA The Threat of Electronic Consumer Goods to National Cybersecurity - Michigan Journal of Political Science A Taxonomy of Hardware Trojans in Printed Circuit Boards - Ohio State University DCSA CI Threat to Electronics - DCSA A survey of hardware Trojans: The payloads, taxonomy, and detection - ScienceDirect PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure - CISA Volt Typhoon Threat Brief - Palo Alto Networks Unit 42 China - CISA Volt Typhoon - Wikipedia Volt Typhoon: Living Off the Land for Cyber Espionage - Picus Security What is Volt Typhoon? A cybersecurity expert explains the Chinese hackers targeting US critical infrastructure - UMBC Recent Supply Chain Attacks Examined - CyberInt Supply Chain Attacks You Can Learn From - ReversingLabs DHS: Imported tech tainted with backdoor attack tools - CSO Online Building a Resilient Ecosystem - DNI.gov Supply Chains Are the Next Subject of Cyberattacks - Global Supply Chain Law Blog Pwned on arrival: How governments can tamper with hardware before you even buy it - The Privacy Issue Trade Wars: US Tariffs and Cyber Risk - SecureWorld Top 10 Supply Chain Attacks - Cisco Outshift A Timeline of Software Supply Chain Attacks - Sonatype Russia - CISA The Nefarious Five: Top Russian State-Sponsored Cyber Threat Groups - NetSecurity Cyberwarfare by Russia - Wikipedia Unpacking Russia's cyber nesting doll - Atlantic Council CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF - Defense.gov The Five Bears: Russia's Offensive Cyber Capabilities - GreyDynamics FBI PSA: Russian Government Cyber Actors Targeting Networking Devices - AHA DHS warns smuggled Chinese jammers pose growing threat - The Washington Times Chinese Signal Jammers Pose a Threat to Police and First Responder Drones - DroneXL Cell Phone Jamming Technology for Contraband Interdiction in Correctional Settings - Urban Institute 2024 United States telecommunications hack - Wikipedia Salt Typhoon: Implications and Strategies to Address Heightened Security Risks - Alvarez & Marsal Grassley to Charter Communications - Salt Typhoon Hack - Senator Chuck Grassley 'Salt Typhoon' Exposes U.S. Cyber Vulnerabilities - ITIF What is Salt Typhoon? A security expert explains the Chinese hackers and their attack on US telecommunications networks - UMBC Nation-State Cyber Actors - CISA Crypto Social Engineering: North Korean APTs in 2024 - CyberProof Groups - MITRE ATT&CK APT Groups - Google Cloud Hardening U.S. Infrastructure Before a Potential Iranian Cyber Attack - ITIF APT Groups: A List of Known Advanced Persistent Threats - Varonis Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups - U.S. Department of the Treasury The Dangers of Counterfeit Items - ICE Combatting Counterfeit Threats - Retronix Government Responses to Counterfeit Parts - ERAI Counterfeit Parts - Defense Acquisition University The Global Impact of Counterfeit Parts - Element Defense Counterfeit Materials Undermine Armed Forces - ACT Power Ransomware Impacting U.S. County Governments - FBI IC3 Foreign

Cyber Threats to the United States: A Primer - Congressional Research Service Thousands impacted by cyberattacks in three states and Puerto Rico - The Record Municipalities Cybersecurity Report - KnowBe4 The Underbelly of Ransomware Attacks on Local Governments - Council on Foreign Relations Securing Cities: The Fight Against Local-Level Cyberthreats - Domestic Preparedness The Increase in Ransomware Attacks on Local Governments - SecurityScorecard Cybercriminals hit Orleans-area sheriff's office with ransomware attack - Yahoo News Cybersecurity in local governments: A systematic literature review - ScienceDirect Backdoor Trojans in Imported Technology - DTIC China PLA Unit Purchasing Antivirus for Exploitation - Recorded Future Purposefully Manufactured Vulnerabilities in Microchips - Naval Postgraduate School Hackers Target Government Defense Contractors With New Backdoor Malware - US Cloud China's Cyber Capabilities - U.S.-China Economic and Security Review Commission