Stranger Pings

The Threat of CCP-Controlled Infrastructure in the U.S. Communications Backbone

---

THE SELECT COMMITTEE ON THE STRATEGIC COMPETITION BETWEEN THE UNITED STATES AND THE CHINESE COMMUNIST PARTY

Table of Contents

Executive Summary

In the fall of 2024, the "Salt Typhoon" campaign—a cyber-espionage operation directed by the People's Republic of China (PRC)—infiltrated the core of America's telecommunications backbone, breaching the networks of multiple major American telecommunications companies and internet service providers. The attackers bypassed traditional perimeter defenses to access systems enabling them to steal call-records data, compromise sensitive private communications of some individuals, and exploit sensitive law enforcement information.[1] This operation proved that Beijing's hackers no longer rely on malware alone. Instead, they weaponize the fundamental architecture of carrier networks—routing, reachability, and trusted pathways—to maintain deep, persistent access and evade detection.

The U.S. government recognized this threat years earlier, when the Federal Communications Commission (FCC or Commission) took the critical step of revoking or denying the Section 214 authorizations[2] of China Telecom (Americas) Corporation, China Mobile International (USA) Inc., and China Unicom (Americas) Operations Limited to block them from providing retail telecommunication services. However, those administrative actions did not require these Chinese telecommunication providers to shut down all physical operations in the United States. The carriers quietly obtained or retained hardware, interconnection agreements, and data center footholds that served as their "trusted" backdoors.

This House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Select Committee) investigation identifies four ways this residual footprint could have facilitated the Salt Typhoon assault and leaves open the door to future cyber operations against the United States:

1. **PRC telecommunications firms operating in the United States do not act independently.** Core routing, provisioning, compliance, and customer-visibility functions remain tied to parent and affiliate systems in the PRC, leaving operations within Beijing's reach.

2. **The carriers kept trusted positions inside U.S. communications infrastructure.** They retained points of presence,[3] routers, and interconnection arrangements in major domestic data centers and internet exchange points.

3. **PRC state-controlled actors can use that footprint to preserve access and hide activity.** From trusted U.S. network nodes, they can keep infrastructure reachable, steer traffic through preferred paths, mask origin, and maintain backup routes when defenders block known channels.

4. **One PRC telecommunication provider included an "Acceptable Use" Policy in contracts with U.S. companies.** This prohibited the broadcasting of political news against state laws of the PRC, the broadcasting of information in violation of PRC state security laws, and the broadcasting of information in violation of the "social order and social stability."

To close this gap, the Select Committee recommends building on prior bipartisan actions and pursuing the following policies:

1. Codifying the FCC's authority to deny blanket authorizations and domestic interconnection.

2. Establishing statutory authority over retained foreign-adversary infrastructure.

3. Broadening Team Telecom and Information and Communications Technology Services (ICTS) jurisdiction over private commercial arrangements in order to review foreign adversary-controlled infrastructure.

4. Mandating entity-specific FCC Covered List determinations and funding a targeted "rip-and-replace" program.

5. Funding security upgrades that protect internet traffic as it moves through different networks and ensuring the federal government and private sector have the talent they need to address PRC cyber threats.

6. Requiring temporary logging and oversight of anomalous behavior pending reconciliation, removal or mitigation.

Overview

U.S. regulators have long warned that PRC state-owned telecommunications carriers operating in the United States present a severe national security threat. Between 2019 and 2022, the Federal Communications Commission (FCC) denied or revoked the Section 214 authority of China Telecom (Americas) Corporation (CTA), China Mobile International (USA) Inc. (CMI USA), and China Unicom (Americas) Operations Limited (CUA) after finding that each company was vulnerable to Chinese Communist Party (CCP) exploitation, influence, and control.[4] Those critical actions barred the companies from providing covered telecommunications services, but they did not require them to remove their physical presence in the U.S., terminate their network relationships, or exit the U.S. internet infrastructure ecosystem.

That unresolved regulatory gap became more urgent following public U.S. government reporting on cyber activity by actors affiliated with the People's Republic of China (PRC) against American telecommunications networks. In November 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) confirmed that PRC-affiliated actors had compromised multiple telecommunications companies, stolen customer call-record data, accessed the private communications of targeted individuals, and copied information subject to U.S. law-enforcement court orders.[5] Subsequent guidance from CISA, the National Security Agency (NSA), the FBI, and allied international partners further documented PRC state-sponsored targeting of telecommunications and critical infrastructure networks globally, most notably through the "Salt Typhoon" intrusion campaign.[6]

Against that backdrop, the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Select Committee) launched an expansive investigation to address national security concerns about CTA's, CUA's, and CMI USA's residual operations in the United States, including the threat posed to the security and privacy of Americans' communications and networks. A key element of this inquiry was whether these residual operations created a dangerous regulatory blind spot allowing them to remain embedded inside the U.S. internet ecosystem through services completely outside the Section 214 licensing regime.

The Select Committee's inquiry commenced on March 5, 2025, with a bipartisan hearing titled *End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses*.[7] The following day, Chairman John Moolenaar and then-Ranking Member Raja Krishnamoorthi sent letters to the

chief executives of China Mobile International Limited, China Telecom (Americas) Corporation, and China Unicom (Americas) Corporation, requesting documents bearing on their respective network infrastructure, customer relationships, and compliance with prior FCC orders.[8] When all three PRC carriers failed to produce responsive materials in the face of PRC Government statements condemning the investigation,[9] the Chairman and Ranking Member sent additional correspondence affirming the information and document requests, accompanied by subpoenas issued by the Select Committee on April 23, 2025.[10] These subpoenas were condemned by the PRC Government's *Global Times* in an April 24, 2025 article.[11]

After reviewing the companies' productions and rejecting the PRC Government's pushback, bipartisan Select Committee staff conducted eight transcribed interviews under oath from September 10 through September 30, 2025. The witnesses represented all three subject companies and spanned a range of operational functions, including network engineering, data center infrastructure, service provisioning, legal compliance, and network operations management. Their willingness to be forthright with the Select Committee was similarly varied, with some witnesses appearing to answer questions in good faith and others claiming ignorance of basic facts. The Select Committee anonymized the names of the witnesses given their roles and responsibilities within each company.

The Select Committee also supplemented the testimonial and document record with four technical datasets spanning January 2018 through June 2025: Border Gateway Protocol (BGP)[a] routing records,[12] federal records,[13] Cloudflare's database of confirmed BGP hijack events,[14] and Shodan and Censys network infrastructure scans.[15] The Select Committee evaluated the technical record conservatively, refusing to treat every routing anomaly as definitive proof of malicious intent, successful exfiltration, data decryption, or knowing complicity by U.S. subsidiary personnel.

Even under that conservative standard, the record established the core conclusion of this report: the FCC's Section 214 actions were essential, but CTA's, CUA's, and CMI USA's persistent operations in the United States present a distinct threat to our national security that must also be immediately addressed. While these companies lost authority to provide covered telecommunications services, existing law did not require them to remove infrastructure or terminate peering or interconnection relationships. Nor did it require them to pull out of colocation arrangements—the practice of renting space, power, and cooling to host their own hardware in third-party data centers—or to cease the internet and internet protocol (IP)-management services that rely on the same underlying assets. As a result, Chinese state-owned carriers remained deeply embedded in the U.S. internet ecosystem long after federal regulators had already found them

[a] BGP is the internet's foundational system for directing traffic between different networks, the large-scale manipulation of which is examined in Part III.

vulnerable to CCP exploitation, influence, and control and took action to terminate their provision of international telecommunication services.

This report outlines three foundational findings demonstrating why that retained presence remains a national security risk:

- **Finding 1:** China Telecom's, China Mobile's, and China Unicom's U.S. subsidiaries are not truly independent from their PRC and Hong Kong parent companies.

- **Finding 2:** The FCC's actions limit what services CTA, CUA, and CMI USA can sell, but do not remove their equipment, data center presence, or network relationships from the United States.

- **Finding 3:** Because China Telecom's, China Mobile's, and China Unicom's subsidiaries and affiliated networks remain embedded in U.S. internet infrastructure, their PRC-controlled parent systems create security and privacy risks for U.S. internet traffic.

Following these findings, the final section explains why existing legal authorities should be expanded to address this threat and recommends concrete legislative reforms to prevent foreign adversary carriers from retaining operational access to U.S. networks after losing telecommunications authority.

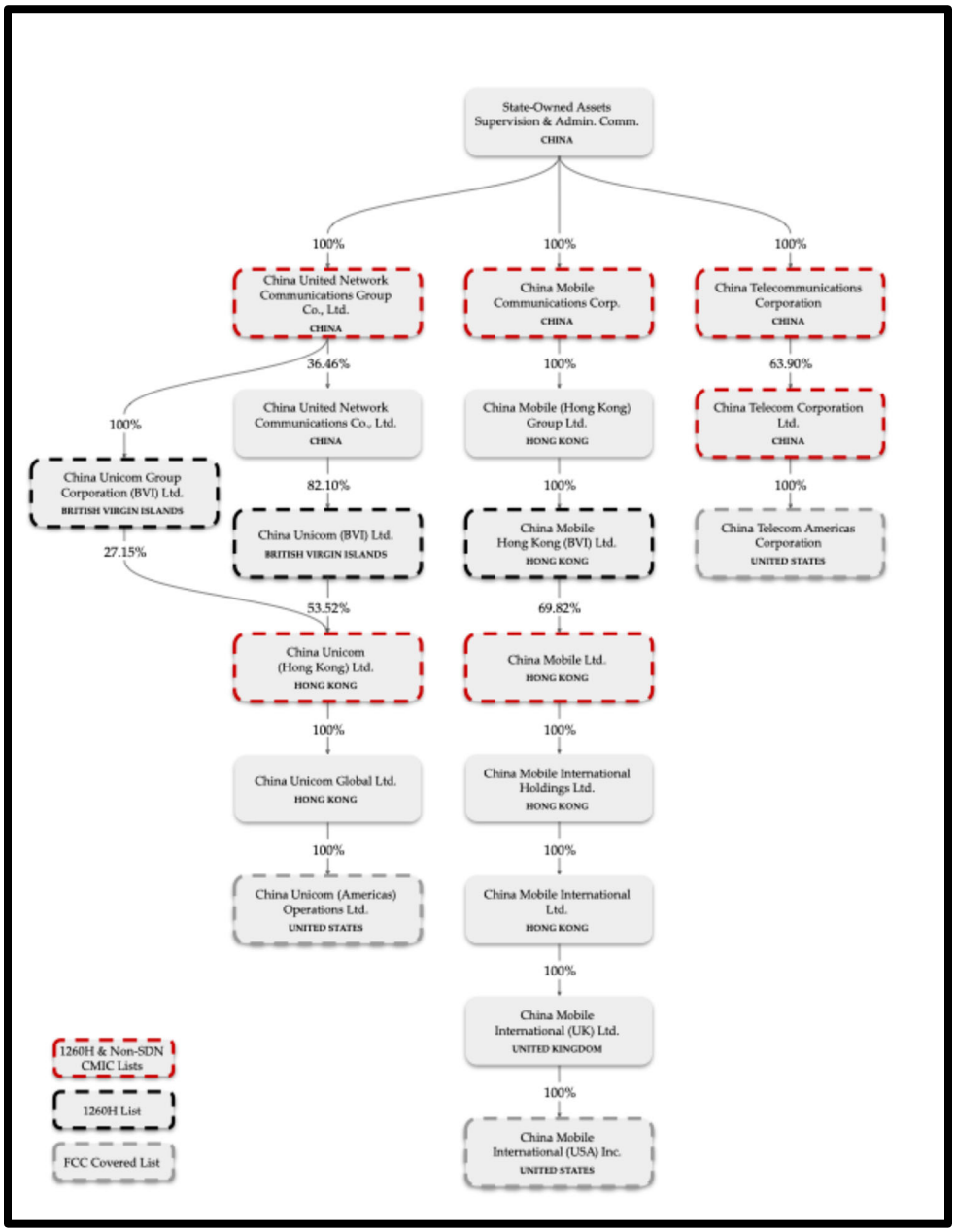
Part I. Parent Direction and Control of the U.S. Subsidiaries

The Select Committee found that all three U.S. subsidiaries lacked meaningful independent control over key corporate and operational functions. Parent or affiliate entities in the PRC or Hong Kong retained authority over compliance systems, customer visibility, service approvals, provisioning, troubleshooting, and network operations. Across all three companies, the pattern was consistent: the U.S. subsidiaries operated as domestic-facing entities, while core decision-making and operational authority remained tied to parent or affiliate entities outside the United States.

A. Corporate Ownership

The FCC and the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (Team Telecom) reached the same basic conclusion across the relevant proceedings: these U.S. entities were domestic corporations ultimately subject to PRC state ownership, influence, or control through their Chinese state-owned parent companies.[16] China Telecom (Americas) Corporation (CTA), China Mobile International (USA) Inc. (CMI USA), and China Unicom (Americas) Operations Limited (CUA) each sit at the bottom of an ownership chain that runs through Hong Kong and offshore holding companies to a Chinese state-owned enterprise. In each case, the relevant parent enterprise is supervised by the State-owned Assets Supervision and Administration Commission of the State Council (SASAC), the PRC government body that exercises ownership rights over central state-owned enterprises on behalf of the state.[17] No independent U.S. ownership interest interrupts any of the three chains, as Figure 1 traces in full.

Figure 1: Ownership Diagram



The China Unicom chain illustrates how PRC control persists through a layered corporate structure even when public shareholders are present. Although China Unicom (Hong Kong) Limited is publicly listed, its ultimate holding company remains China United Network Communication Group Company Limited. This larger entity is a PRC state-owned enterprise. In a 2018 joint application before the FCC, China United Network Communication Group Company Limited and its co-applicants disclosed that SASAC directly held a 96.5 percent voting equity interest in the parent company, leaving the corporate group under ultimate PRC state control notwithstanding minority public

ownership at the listed-company level.[18] Yet when a senior CUA legal and compliance officer was questioned by the Select Committee about whether the relevant parent company was state-owned, he responded that he did not know.[19] While possibly an issue in its own right, state control is all the more concerning when a company's senior compliance officials will not or cannot acknowledge a simple fact disclosed in the company's own filings.

The national security judgment underlying these chains extends well beyond the FCC's licensing authority. The Department of Defense (DoD) lists China Telecom Group Co., Ltd., China Mobile Communications Group Co., Ltd., and China United Network Communications Group Co., Ltd.—together with certain of their Hong Kong and British Virgin Islands affiliates—as "Chinese military companies" operating in the United States under Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.[20] The Department of the Treasury lists the same three parents on its Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List under Executive Order 14032, which restricts U.S. investment in companies tied to the PRC's military-civil fusion strategy.[21]

Crucially, PRC national security laws require all three parent carriers to hand over data upon state demand, including by virtue of the National Intelligence Law that requires PRC entities to "support, assist, and cooperate with national intelligence efforts."[22] That legal obligation follows the network infrastructure globally. Because the U.S. subsidiaries rely on parent-controlled routing and systems, any query, prompt, or output traveling over infrastructure managed by these entities—whether transmitted by a student, a commercial developer, or a corporate laboratory—remains potentially visible to Chinese intelligence services. In short, the physical wires and digital pathways operating in the United States function as legal extensions of the PRC security state.

B. Corporate Governance and Compliance Blind Spots

The most direct corporate governance evidence concerns CUA. In response to a congressional subpoena, CUA disclosed that seven of the board's eight directors are CCP members and that two of the three senior management team members are CCP members.[23] At the same time, the company represented that there were no agreements with PRC government entities, no formal or informal government requests, no military or defense engagement, and no internal CCP committees.[24] Those representations sit beside a board and senior management structure dominated by CCP members.

CUA also operated on parent-controlled information technology and policy systems. U.S.-based employees used Chinese email addresses and accessed internal records through a VPN into parent-controlled systems. Evidence indicates that they operated under cybersecurity, administrative, and privacy policies issued by China Unicom Global (CUG).[25] When asked where policy templates originated, Witness 5 answered:

> "The template proposed and issued by CUG, our parent company."[26]

That testimony shows that CUA did not independently generate the policies governing major parts of domestic operations. Parent-issued templates shaped the subsidiary's cybersecurity, finance, administration, and privacy posture.[27]

Separately, issues with the compliance gap became clearest when Witness 5 explained that CUA could agree for itself to comply with U.S. law, but could not make the same guarantee for CUG:

> "We cannot guarantee the affiliate, specifically the CUG, to comply with U.S. laws."[28]

That statement shows that the U.S. subsidiary depended on parent-controlled systems, templates, and network relationships, but could not guarantee that the parent entity supporting those operations complied with U.S. law.

CUA also lacked visibility into the ultimate customers and uses of some services. The PRC-based parent could direct the U.S. subsidiary to provision servers and connectivity for unidentified parties without disclosing who the ultimate beneficiaries were or how the infrastructure would be used.[29] When asked whether CUA had no idea who the third-party recipients of the provided services in China were, Witness 5 answered: "Yes."[30] When pressed on whether CUA sought to learn the identities of the beneficiaries of its services in the PRC, to ensure it did not provide services to entities which may be sanctioned or otherwise prohibited by the U.S. Government, he responded:

> "I do not ask the third-party's name. . . ."[31]

When asked additional questions about how a compliance official of the U.S. subsidiary can claim to ensure American legal compliance without even basic visibility into the identity of those in the PRC who benefit from its services, he explained:

> "That's the obligation of [PRC parent] CUG. Because CUG signed the contract or is the end customer in China, they need to, you know, make sure to [be] complying with the U.S. law. As for [the American subsidiary] CUA, we provide the service to CUG."[32]

That practical visibility gap creates an operational accountability problem. The U.S. subsidiary could help provide access to U.S. infrastructure without knowing who ultimately used the service or for what purpose. Indeed, hypothetically, a PRC intelligence agency itself could contract for services in the U.S. with the parent company and the U.S. subsidiary would remain ignorant of this reality. This is an unacceptable blind spot.

C. Parent-Directed Network Operations

A primary example of parent direction appears in network availability. Witness 3 confirmed that CTA receives "freeze notifications," or administrative pauses on non-essential network changes or maintenance, from the parent entity whenever there is a major event or holiday in the PRC, and that the freezes apply across the customer base:

> "It's not about a particular customer—it applies to all customers."[33]

That testimony shows that parent-controlled freezes could affect provisioning and network-change activity for U.S. customers based on the PRC parent's event or holiday calendar, rather than the independent discretion of the U.S. subsidiary.[34]

CTA's Network Operations Center (NOC), the centralized facility where network performance is monitored and managed, and ticketing structure showed the same dependency. Witness 4 confirmed that CTA has a continuous NOC function, but described a workflow in which troubleshooting and engineering functions run through Shanghai and Hong Kong.[35] Customer trouble tickets are first logged by a call center in Shanghai. Tickets involving international circuits are forwarded to CTG's NOCs in Hong Kong or Beijing. The U.S. NOC handles only domestic circuits.

CTA also confirmed that the subsidiary keeps no independent traffic-flow logs.[36] That limits the American subsidiary's ability to detect, verify, or reconstruct whether parent or affiliate entities altered routing involving network assets on U.S. soil.

CTA provides direct evidence of two-way provisioning, troubleshooting, and network-change authority that is controlled in China. Service orders, or formal requests for network infrastructure or service activation, were centrally managed through parent-company systems. Witness 3 explained that CTA project managers place orders with Shanghai Telecom through an internal customer relationship management (CRM) system and that no separate contract is needed for Shanghai Telecom to implement the order:

> "We don't need a contract with Shanghai Telecom. We would input information about the order into an internal system…and the order will flow to Shanghai Telecom, and Shanghai Telecom will implement it."[37]

In other words, Shanghai Telecom has direct access to files and orders coming to CTA without a separate agreement between CTA and the entity carrying out the work.

China Mobile USA provides similar operational-dependency evidence. Witness 1 described CMI USA as a sales-oriented presence:

> "CMI USA is basically a sales team."[38]

That description was consistent with the company's technical structure. CMI USA did not operate as a standalone U.S. network company with its own engineering function. The FCC denied China Mobile USA's Section 214 application in 2019 explaining that, "China Mobile USA is a Delaware corporation that is indirectly and ultimately owned and controlled by the Chinese government. China Mobile USA is an indirect but wholly owned subsidiary of China Mobile Limited, a Hong Kong entity that is publicly traded on the New York and Hong Kong exchanges…China Mobile Hong Kong (BVI) Limited, a British Virgin Islands investment holding company, owns over 70% of China Mobile Limited. China Mobile Hong Kong (BVI) Limited is ultimately 100% owned by China Mobile Communications Corporation (China Mobile), which is 100% owned by the Chinese government. China Mobile is a state-owned enterprise subject to the supervision of the State-Owned Assets Supervision and Administration Commission, a Chinese government body."[39] After the denial, China Mobile International maintained a U.S. network footprint through technical assistance to CMI USA. Witness 2 explained, "We don't have network engineers."[40b]

Witness 1 explained that Hong Kong headquarters reviews orders through the internal system and that the headquarters commercial center assesses and approves them before local suppliers provision the space.[41] Crucially, Witness 1 acknowledged that CMI USA does not monitor customer usage patterns, does not investigate suspicious activity, and does not track what services customers run on the infrastructure it arranges.

When Select Committee investigators asked about U.S.-based network staff, witnesses could not identify a single network operating team outside Hong Kong. Witness 1 stated:

> "I have never heard any other operating team outside of Hong Kong."[42]

Communications with headquarters ran through email, WeChat, and an internal platform, and often required U.S.-based staff to communicate late at night because of the time difference. Together, that testimony shows that CMI USA's infrastructure was commercially managed within the United States but operationally controlled through CMI and headquarters personnel abroad.

[b]CMI USA maintains that it had a US defense contractor as a third-party to monitor traffic for security through 2022.

Part II. Retention of Unregulated U.S. Infrastructure & Network Relationships

The FCC's Section 214 revocations and denials did not physically remove CTA, CUA, or CMI USA from the U.S. internet infrastructure ecosystem. This enduring loophole exists because a Section 214 order is strictly a commercial sales license, not a physical eviction mechanism. The current statute merely dictates that "[n]o carrier shall undertake the construction of a new line," "acquire or operate any line," or "engage in transmission" without an FCC certificate of "public convenience and necessity."[43] Revoking this authority terminates a carrier's legal right to sell regulated telecommunications services, but it exercises no control over private property ownership, hardware deployments, or facility leases.

Consequently, the FCC's admirable and historic enforcement actions addressed only a fraction of the national security threat. The CTA revocation order, for example, strictly directed the company to "discontinue all services relating to its section 214 authority" within sixty days.[44] In practical terms, losing a Section 214 authorization is like a commercial trucking company losing its public common-carrier license to run standard transit routes. The company can no longer legally sell those public transport services, but it retains full ownership of its physical warehouses, keeps its trucks parked inside with the engines idling, and remains entirely free to use those exact same assets to fulfill unregulated private logistics contracts.

Because of the statutory limits of Section 214, this language targeted only services tied to that specific commercial license, leaving the underlying physical and technical infrastructure entirely untouched.

In light of this, the FCC recently proposed to exclude Covered List entities from blanket domestic Section 214 authority, to consider revocation or deemed revocation of existing blanket domestic authority, and to prohibit telecommunications carriers from interconnecting with Covered List entities absent prior FCC authorization.[45] The FCC also sought comment on whether that prohibition should extend to facilities, including Points of Presence and data centers, owned or operated by Covered List entities, and whether holders of Covered Authorizations should be restricted from transactions or other dealings with entities whose international Section 214 authority had been revoked or denied on national security grounds.

Notwithstanding these proposals that validate the physical and logical security risks documented in this report, there remains a significant legislative gap. While the FCC's pending notice of proposed rulemaking (NPRM) explores the outer limits of its authority under Sections 214, 201, and 251, it remains an incomplete fix. It does not create a durable statutory removal program, provide the necessary appropriations, or grant the FCC the standalone authority needed to reach the full breadth of colocation, routing, remote operations, and non-licensed

services footprint documented in this report.[46] Ultimately, while this proposed regulatory expansion represents a critical first step in closing the physical interconnection loophole, it serves as the necessary foundation for addressing the broader, multi-layered risk environment that continues to exist.

An examination of subpoenaed records and network data reveals that these carriers continue to exploit these regulatory gaps across some or all of five distinct vectors that progress from commercial form to operational control. The vectors are (1) the commercial pivot to unregulated network services, (2) the retention of strategic physical footprints inside premier U.S. carrier hotels, (3) the continued operation of Chinese-manufactured network hardware, (4) the maintenance of trusted logical routing identities tied directly to parent backbones in the PRC, and (5) the imposition of PRC-directed acceptable use terms on U.S. customers.

A. The Commercial Pivot to Unregulated Network Services

Section 214 governs only regulated common-carrier telecommunications, the specific services for which the FCC issues operating certificates. Because it does not function as a comprehensive exit order, it does not automatically sever every internet, interconnection, data center, cloud-connectivity, or enterprise-network relationship a carrier may maintain. All three PRC state-controlled carriers actively pivoted into this less-regulated network-services market. By rebuilding their U.S. businesses around network services outside the core Section 214 licensing framework, they preserved their operational footing at critical nodes of U.S. internet infrastructure.[47]

Specifically, these subsidiaries continue to market, resell, or support varying combinations of the following enterprise network offerings:

- **IP Transit & Interconnection:** Routing customer data across the global internet and bridging traffic between U.S. networks and mainland China or Hong Kong backbones.
- **Colocation & Data Center Services:** Renting secure physical space, power, cooling, and direct cross-connects inside U.S. facilities.
- **Enterprise Networking:** Managed Multi-Protocol Label Switching (MPLS) VPNs, which route enterprise traffic through provider-managed logical paths, a legacy technology that creates private, predictable, and secure connections across wide areas, and Software-Defined Wide Area Networks (SD-WANs), which manage traffic across geographically distributed locations using software to dynamically route traffic over multiple transport types (e.g., broadband, LTE, or MPLS) to optimize performance.
- **Resale and Systems Integration:** Brokering third-party network equipment, maintenance, and support services for enterprise customers, including vendor support contracts for U.S.-based network infrastructure.

Subpoenaed documents from all three carriers demonstrate how this commercial pivot unfolded in practice, keeping their operations deeply embedded in U.S. networks.

First, after its Section 214 revocation, CTA restructured rather than withdrew, telling the Select Committee that it "currently provides exclusively enterprise and carrier business services in the U.S." and acknowledging that its internet access and transit services depended on "the IP networks in the United States."[48] The carrier disclosed 35 active agreements for services touching U.S. soil,[49] with customers across many sectors including, but not limited to, energy, mining, cyber, financial, and political.[50] Supplier-side agreements also show CTA plugging directly into the domestic internet's physical architecture, procuring transit, private-line, Ethernet, colocation, and cross-connect arrangements from major Western carriers.[51] Furthermore, internal agreements formalized CTA's role as a procurement pipeline for its Beijing-based parent, with a 2007 agreement authorizing each entity "to provide or procure Services" for the other party and "for use by persons who contract directly with that Party,"[52] and a 2016 agreement requiring CTA to "procure services from third-party providers" and transfer those services to CTCL's Global Business Department.[53]

Second, CUA leveraged ordinary market demand to retain major enterprise clients. CUA's records reveal contracts with U.S. technology companies for private leased circuits, paid peering, IP transit, CDN services, and cross-connects.[54] These services gave customers direct access to China Unicom's global routing ecosystem, including China- and Asia-facing paths through AS10099 and AS4837.[55] However, this access came with significant strings attached. CUA's Dedicated Internet Access terms required users to provide network-usage information, including IP addresses and domain names, to "receive the review of the telecom department," and exposed them to the loss of assigned IP addresses or "service termination" for violations.[56] Consequently, CUA fulfilled legitimate connectivity needs while maintaining a carrier foothold equipped with PRC-style reporting and termination leverage, which Section E demonstrates was a formal, contractually mandated "acceptable use" requirement.

Third, CMI USA remained active in the United States as a network middleman, acting as a reseller and systems-integration broker. Despite telling the Select Committee it operated only passive "meet me" points for routing traffic, regulatory records show CMI USA actively resold enterprise connectivity and data center services to a sprawling roster of PRC-based companies,[57] as well as PRC Government entities.[58] CMI USA also sold IP Transit to a cluster of small PRC-linked cloud and hosting resellers, forming a transit channel into China-affiliated hosting infrastructure.[59] It also sold transit to PRC-linked cloud resellers and routed U.S. Internet Data Center capacity intra-group to its state-owned parent's provincial branches in China.[60]

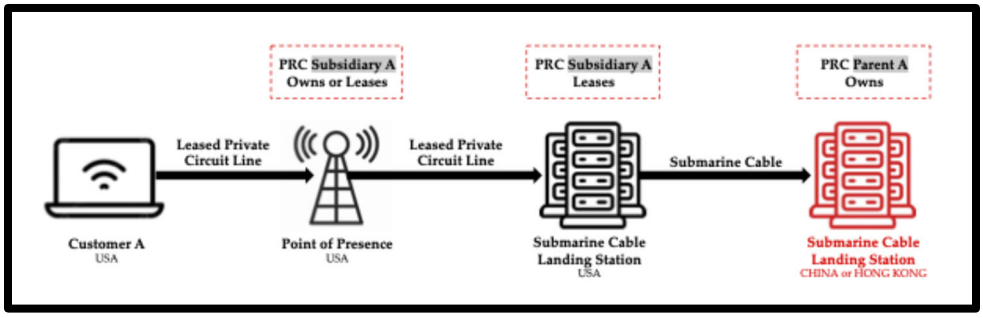
Operating parallel to this reseller business, CMI USA "procur[ed] internal network components for enterprises," including U.S. subsidiaries of Chinese companies.[61] These procurements included servers, switches, firewalls, optical

transceivers, and fiber cables for customers in Michigan and California.[62] In several transactions, CMI USA purchased this equipment through a "supplier relationship" with ECCOM Network (USA), Inc. ("ECCOM USA").[63] ECCOM USA is an indirect U.S. subsidiary of Shanghai-based ECCOM Network System Co., Ltd. ("ECCOM"), itself a subsidiary of CETC Digital Technology Co., Ltd. ("CETC Digital"), the listed arm of China Electronics Technology Group Corporation ("CETC").[64] CETC is a PRC state-owned defense conglomerate designated by the Department of Defense as a Chinese military company and listed by Treasury as a Non-SDN Chinese Military-Industrial Complex Company.[65] In effect, CMI USA placed the U.S.-based subsidiary of a designated PRC military company in the procurement chain for network equipment deployed at U.S. enterprise facilities.

B. The Companies Retain a Physical Presence Inside U.S. Facilities

The carriers retained more than a token presence in the United States. The subpoena productions documented geographically distributed points of presence, colocation space, power, cages, racks, cross-connects, and carrier-capacity arrangements inside the facilities that form the physical nerve centers of the U.S. internet. Although the FCC actions differed by company, the practical result was similar: each carrier or affiliate retained U.S.-based infrastructure relationships outside a simple license-removal framework. Figure 2 illustrates how these retained pieces fit together. For example, Figure 2 shows a U.S. customer's traffic crossing subsidiary-owned equipment and leased circuits before terminating on parent-owned infrastructure in the PRC. Whether the infrastructure is leased or owned, control is what facilitates impact.

Figure 2: Unregulated Private Leased Circuit Architecture



CTA's 2025 production to the Select Committee identified ten active points of presence (PoPs) across seven U.S. metro areas known for their concentration of data centers, submarine cable landings, or both: Ashburn, VA, Chicago, IL, Hillsboro, OR, Los Angeles, CA, Miami, FL, New York, NY, and San Jose, CA. CTA stated that it "only owns network equipment in the PoPs"[66] with sites located in facilities operated by U.S. and PRC digital infrastructure companies.[67]

CUA had the most extensively documented footprint. Witness 6 confirmed that the company owned equipment at leased facilities, and Witness 7 described roughly ten data centers after two closures.[68] The company's representations to the Select Committee document active colocation cages, power allocations, and live cross-connects across Ashburn, Chicago, Dallas, Hillsboro, Los Angeles, Miami, New York, Reston, San Jose, Seattle, and Palo Alto among various providers.[69] Notably, CUA retained active interconnections with major U.S. backbone providers.[70]

CMI USA's posture was different because the FCC denied China Mobile USA's Section 214 application before the company received authority to provide covered international common-carrier services.[71] Even so, CMI USA's records identified 39 U.S. PoP entries across 27 distinct data center and interconnection facilities operated by U.S. digital infrastructure companies.[72] This vast physical footprint allows the company to bypass the regular public internet and handle staggering amounts of data. Anchored inside major internet hubs across Los Angeles, New York, and Chicago, CMI USA commands an immense total network capacity of up to 1,380 gigabits per second.[73] An internal interconnection inventory produced by the company details how the company uses its physical presence inside these facilities to plug directly into global telecom backbones, public data exchanges, and the private networks of major American tech giants operating right next to them.[74] This is consistent with the Select Committee's Shodan scans at the time, which identified at least 143 active China Mobile network assets across U.S. facilities.[75]

Furthermore, the PRC parent carriers repeatedly sought ownership stakes in trans-Pacific cables that would land on U.S. soil, and U.S. national security objections unwound each one. CMI Limited joined multiple large U.S. technology companies in 2018 as a founding member of the Bay to Bay Express Cable System, allocated fiber pairs and a terrestrial run from a Grover Beach, California landing to a point of presence in San Jose, but the U.S. landing never won FCC approval and CMI Limited divested its interest in 2021.[76] China Telecom and China Unicom pursued the same goal through the Hong Kong–Americas cable, a six-fiber-pair system that would have connected Hong Kong directly to landings at Hermosa Beach and Manchester, California, with each carrier owning a fiber pair.[77] That consortium ultimately withdrew its FCC cable landing license application in March 2021 under the same U.S. government pressure against direct U.S.–Hong Kong links.[78] The broader record shows the same outcome across project after project, including the Pacific Light Cable Network and SeaMeWe-6, as Washington moved to block or unwind PRC-carrier ownership of cables terminating in the United States.[79] Public reports note the potential for the "tapping of cables for the purpose of espionage."[80]

Notably, all three footprints converged on the same interconnection choke points. These carrier hotels are built for global interconnection, concentrating the routing, switching, cross-connect, and peering infrastructure where large volumes of U.S. and international traffic are handed off. A carrier with equipment, live cross-connects, transit relationships, or routing control at these sites may gain

visibility into traffic flows and metadata, create opportunities to divert or intercept traffic, or introduce disruption through deliberate action, compromise, or misconfiguration.[81]

C. Retained Chinese-Manufactured Network Hardware

The carriers also kept Chinese-manufactured equipment running inside U.S. networks, including hardware built by firms subject to PRC legal obligations that can compel cooperation with state security and intelligence services.

Huawei had been CTA's main vendor for transmission equipment, which carries data as light pulses across fiber. CTA's production showed that Huawei equipment remained inside its U.S. PoP footprint, listing Huawei S9303 switches and Huawei OptiX OSN transmission equipment at multiple facilities.[82] Separately, CTA also listed a ZTE ZXR10 switch in CTA's Chicago PoP.[83] The production was consistent with Witness 4's testimony that CTA had replaced roughly 75 percent of its Huawei transmission equipment with Ciena and Nokia, but about 25 percent of the transmission hardware on its U.S. network remained Huawei.[84] Because that equipment sits below many software-based traffic-monitoring tools, a vendor subject to PRC security mandates could be positioned to tap, copy, or disrupt traffic from inside the network without triggering standard intrusion alarms.

The problem extends beyond the big carrier hotels. Network scans reviewed by the Select Committee found active Huawei devices registered to China Mobile operating in Bakersfield, California, well outside the major metropolitan data centers.[85] The finding places Chinese-manufactured hardware at regional aggregation points around the country, not only at the central interconnection hubs. Wherever that gear handles U.S. traffic, it runs closed firmware the operator cannot fully see into, leaving a path for interception or disruption that ordinary monitoring would miss.

The equipment-layer risk is not limited to Huawei or ZTE. Publicly available materials show that Ruijie Networks Co., Ltd. (Ruijie Networks), a Fuzhou-based maker of routers, switches, and wireless access points, has supplied equipment to China Telecom, China Mobile, and China Unicom, including switches, routers, and data center products.[86] Ruijie Networks is a "level 2" technical support unit for the China National Vulnerability Database of Information Security (CNNVD), a status under which the company "signs a cooperation agreement with CNNVD" and helps "elevate China's research in information security vulnerabilities."[87] CNNVD is operated by the China Information Technology Security Evaluation Center (CNITSEC), which Recorded Future has identified as subordinate to the Ministry of State Security and capable of delaying or controlling vulnerability disclosure for intelligence purposes.[88] That arrangement gives an MSS-run body a cooperative relationship with a vendor whose hardware sits inside U.S. carrier networks.[89]

Figure 3: Ruijie Involved Industries Screenshot

The reach of that hardware is measurable. A Select Committee network scan conducted in June 2025 using Shodan identified approximately 6,000 Ruijie Networks devices discoverable in U.S. networks.[90] The equipment also carries documented security exposure. In December 2024, CISA issued advisory ICSA-24-338-01 documenting critical vulnerabilities in Ruijie Network's Reyee cloud platform and operating system, including a flaw permitting arbitrary command execution on affected devices.[91] Network equipment carrying exploitable firmware can copy, redirect, or manipulate traffic from inside the network without triggering the software-based alerts that defenders monitor.

Ruijie Networks of Fuzhou is not currently identified on the FCC Covered List. That means the FCC revocation orders and the pending rulemaking in WC Docket No. 26-82 do not by themselves impact this hardware or the commercial relationships through which it was sold and distributed. The equipment and its documented vulnerabilities therefore illustrate a regulatory perimeter problem: the pending FCC rule is triggered by Covered List status, while this report identifies risk that may arise before the Covered List process has caught up to the technical record.[92]

D. Trusted Network Connections and Routing Identities Tied to the PRC Parents

Physical presence inside a carrier hotel becomes a potential threat vector when a network is configured to trust the entities to which it connects. Subpoenaed productions show that despite the FCC's revocation orders, these trusted connections and parent-linked routing identities remained active at the network layer. This continuity binds U.S.-based hardware directly to parent-company network backbones operating entirely outside independent domestic oversight. The FCC's pending rulemaking has tentatively concluded that telecommunications carriers should be prohibited from maintaining trusted

interconnection relationships with Covered List entities absent prior FCC authorization. If finalized, this would address such relationships in the future to the extent they fall within the FCC's asserted interconnection authority. But the NPRM is not final, and it rests on statutory authorities that could be narrowed by the FCC in the future. Statutory codification would turn that proposed protection into a durable rule of decision.[93]

CUA's U.S. network was configured to trust its Hong Kong parent at the border-router level. Witness 6 confirmed that CUG appeared on CUA's network "allowlist,"[c] a configuration that permits specified traffic or connections from an approved source without standard security screening. Engineering records show that the allowlist applied directly to CUA's border routers. Witness 6 also confirmed that CUA used both static routing and BGP between its PoPs in the same environment in which CUG was allowlisted.[94] BGP, the protocol whose large-scale manipulation Part III examines, therefore operated within the same environment in which CUG was allowlisted.[95] This finding gives technical specificity to the Senate Permanent Subcommittee on Investigations' earlier conclusion that CUA "leverages CUG's network operations center, located in Hong Kong, for technical support," that CUG "monitors CUA's network operations," and that "CUG can remotely configure CUA's network equipment."[96][d]

CTA maintained a parallel vulnerability at the routing layer, ensuring its post-revocation network services remained connected to both domestic and international traffic pathways. CTA acknowledged that it "leases transmission capacity in the United States" from major carriers.[97] CTA also disclosed international arrangements used "to facilitate data transmission from the United States," connecting U.S. network points to foreign endpoints, including Los Angeles to Japan, Chicago and New York to Toronto, and Miami and New York to São Paulo.[98] Finally, CTA stated that it has "free peering arrangements in the U.S. with major ISPs," which "allow CTA to pass its traffic to users of these other networks," and noted that these arrangements are "largely done on a 'handshake' basis without any formal agreement."[99]

Witness 4 confirmed that CTA's U.S. network, operating as Autonomous System (AS) 36678 (AS36678), remained directly connected to CTG, including AS4134, CTG's primary global backbone.[100] An AS is a network or group of networks under the control of a single operator that presents a unified routing policy to the rest of the internet, and its AS number (ASN) is the unique identifier other networks use to direct traffic to it. CTA's U.S.-based infrastructure therefore was not fully separated from the PRC parent network. It retained a direct, trusted

[c] "Allowlists" are a common network administration practice that permit trusted entities to bypass selected filtering or security protocols. However, if traffic originating from a PRC-affiliated network were routed through the Hong Kong parent and recognized under CUG's allowlist designation, that PRC entity could receive the same trusted treatment as CUG.

[d] CUA asserts that it adheres to allowlist standards designed to satisfy MANRS norms. However, CUA is not part of MANRS, or the higher standard and more transparent MANRS+, so the claim is not auditable.

physical routing relationship with CTG at key West Coast interconnection points in Los Angeles and San Jose, preserving a standing pathway for the parent network to execute commands or manipulate traffic from abroad.

China Mobile USA carried the same dependency at the level of routing identity. China Mobile USA did not operate its own autonomous system number for relevant overseas routing. It relied instead on China Mobile International-controlled routing infrastructure, including AS58453.[101] Asked whether "China Mobile U.S. doesn't have their own ASN," Witness 2 answered: "Correct."[102]

By leaving these routing identities, routing relationships, and parent-linked network connections active, the post-revocation ecosystem allowed foreign-adversary parents to maintain direct logical pathways into supposedly restricted U.S. infrastructure.

E. Acceptable Use Policy

The preceding four vectors establish that the carriers retained the physical, technical, and routing capacity to act inside U.S. networks. This fifth vector establishes whose rules govern that capacity. Stripped of the U.S. license that once carried public-interest obligations, at least one of these entities used its unregulated commercial agreements to seek to extend the PRC's own information-control mandates onto their American clients through contract law.

For instance, CUA embedded a mandatory Acceptable Use Policy ("AUP") in IP Transit Agreements with U.S. companies.[103] The specific terms of this policy, as shown below, detail the rigorous censorship and surveillance requirements imposed on U.S. customers.

Figure 4: Acceptable Use Policy

1. No Broadcasting of political news against state laws of People's Republic of China (including the information downloaded from the internet)
2. No broadcasting of state secrets and the information in violation of the state security of People's Republic of China
3. No broadcasting of the information in violation of the social order and social stability, and the information overstating the mass uncontrolled activities and pornography in particular
4. The content over the internet must be approved by the local propaganda agency; No free downloading of the overseas internet content and posting on the domestic websites.
5. Self check on the content management system will have to be conducted, and any problem detected will have to be solved immediately. The information security accountability system will be put in place and the education and review of the content management staff will be strengthened.
6. Be obligated to provide network usage information according to the requirement of China Unicom Americas (e.g. IP address and domain name), fill in the data file required by China Unicom Americas, and receive the review of the telecom department.
7. The user has the right of the use only for the IP address assigned by China Unicom Americas, and has no right of transfer for such IP address, the right of use for the user automatically becomes invalid after the user signs off, the user is obligated to receive the check of the IP address usage by China Unicom Americas. China Unicom Americas has the right to take back the assigned IP address once the user provides faulty data.
8. Various penalties including the service termination will be exercised for any violation for the above rules

Notably, this AUP explicitly requires U.S. customers to adhere to regulatory requirements set by two Chinese state entities: the Ministry of Industry and Information Technology (MIIT) and Ministry of Public Security (MPS).

The MIIT regulates and manages the PRC's telecommunications, software, electronics, and IT manufacturing sectors. It also oversees the PRC's broader defense industry and fits into its broader defense-industrial governance structure through links to the State Administration of Science, Technology and Industry for National Defense (SASTIND) and participation in dual-use export-controls.[104] Meanwhile, the Ministry of Public Security (MPS) serves as the PRC's national police authority, overseeing domestic law enforcement. U.S. government agencies have also identified the MPS as a player in the CCP's transnational repression activities, including efforts to monitor, harass, and influence Chinese dissidents and other targets abroad.[105]

By requiring U.S. customers to comply with requirements issued by these ministries to "strengthen[] the management of information communication in the public information service," CUA effectively sought to export the PRC's internal censorship and surveillance regime into the U.S. market on an extraterritorial basis.[106] The AUP's stated goal—to govern information management and penalize "violations of communication rules"—provided CUA with contractual authority to police its U.S. customers under the direction of the Chinese state.[107]

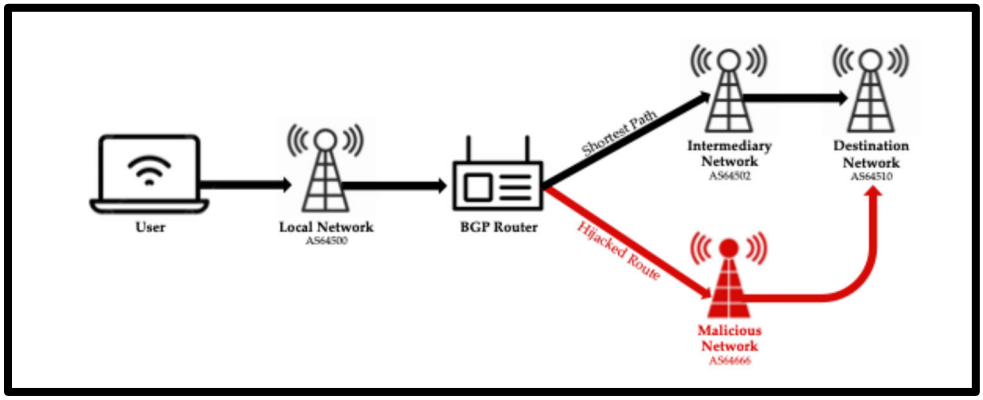
Part III. Routing Exposure Involving U.S. Traffic

With physical infrastructure and trusted network connections secured, these U.S. subsidiaries and their PRC state-controlled parent companies operationalized this access to actively manipulate how American traffic moves across the internet. They accomplished this by exploiting the Border Gateway Protocol (BGP).

BGP is the system that decides how data travels across the global internet. Every network identifies itself with a unique Autonomous System Number (ASN)—the unique identifiers established in Part II—and advertises the range of internet addresses it can reach, prompting intermediate routers to forward messages along the most direct path. In effect, the internet takes networks at their word about which roads they can deliver mail down. The system runs almost entirely on trust. Networks generally accept one another's advertisements without independent verification, assuming that each is telling the truth about the traffic it can carry. Because BGP lacks automatic verification, it is highly vulnerable to exploitation: a BGP hijack occurs when a malicious or compromised network lies to the internet's routing system about which addresses it can reach.[108]

As shown in Figure 5, a bad actor can broadcast a false announcement, claiming that they are the absolute fastest, most direct route to a specific destination. Because the system operates on trust, surrounding BGP routers believe this false announcement and update their internal maps. Like placing a fake detour sign on a highway, the traffic is pulled away from its legitimate path and funneled directly into the hijacker's infrastructure. Once the American data is pulled onto a malicious network, it becomes visible to hostile actors who can copy, monitor, or store the traffic before silently sending it along to its true destination, often without the user ever knowing they were intercepted.[109]

Figure 5: A BGP Prefix Hijack



These carriers are uniquely positioned to exploit network trust. Because Chinese state-owned carriers lack independent transmission facilities outside the PRC, they rely on interconnection agreements with other networks, the exact

arrangements that allow false route announcements to be introduced.[110] The parent-linked routing identities and standing network interconnections detailed in Part II are not merely a residual commercial footprint. They are the active channels through which the hijack announcements described below were introduced.

For over fifteen years, China Telecom and other state-owned carriers have consistently surfaced in technical studies, public reporting, and U.S. Government proceedings regarding large-scale internet routing incidents. These episodes have repeatedly misrouted U.S. government, private-sector, and domestic traffic across PRC-controlled networks.[111]

The earliest well-documented episode occurred on April 8, 2010, when, for roughly eighteen minutes, erroneous routes propagated by China Telecom redirected traffic for about 15 percent of the Internet's destinations through servers in the PRC, affecting U.S. government civilian and military networks, including the Senate, the armed services, the Office of the Secretary of Defense, NASA, the Department of Commerce, and NOAA, along with commercial sites.[112] When ultimately revoking CTA's operating authority, the FCC found that the carrier could "access, store, disrupt, and/or misroute U.S. communications," directly enabling espionage against the United States.[113] Similarly, the Departments of Justice and Defense concluded that China Telecom had continued to exploit BGP vulnerabilities "to misroute United States internet traffic on at least six occasions," exposing that data to interception and alteration.[114e]

The FCC made comparably specific findings about the other two carriers. It determined that CUA could "maliciously or accidentally redirect to China" U.S. data traffic by mounting a BGP route attack from one or more of its eleven U.S. points of presence, and that routing such traffic through China would allow it to be "readily captured, examined, and/or altered."[115] The Commission called that threat "more than theoretical," citing an independent analysis that identified a component of China Unicom as the likely source of more surveillance attacks against U.S. mobile users than any other provider in the world between May 2018 and December 2019.[116]

For China Mobile, the FCC's 2019 application denial confirmed this network-layer threat. Adopting Executive Branch assessments, the Commission concluded that an international Section 214 authorization would grant China Mobile USA direct access to the physical and logical backbone of the U.S. grid. With this infrastructure access, the FCC warned, the carrier would possess the capability to "target, alter, block, and re-route traffic," a danger the Commission directly tied to

[e] The public facing MANRS page represents AS36678 (operated by CTA) as implementing MANRS's four actions. CTA asserts there have been no incidents since joining MANRS. The publicly accessible participant record does not provide enough detail to determine whether AS36678 has experienced routing incidents, how frequently incidents occurred, or how MANRS verified and continuously evaluates the claims.

a documented pattern of Chinese state-backed BGP hijacks against U.S. networks.[117]

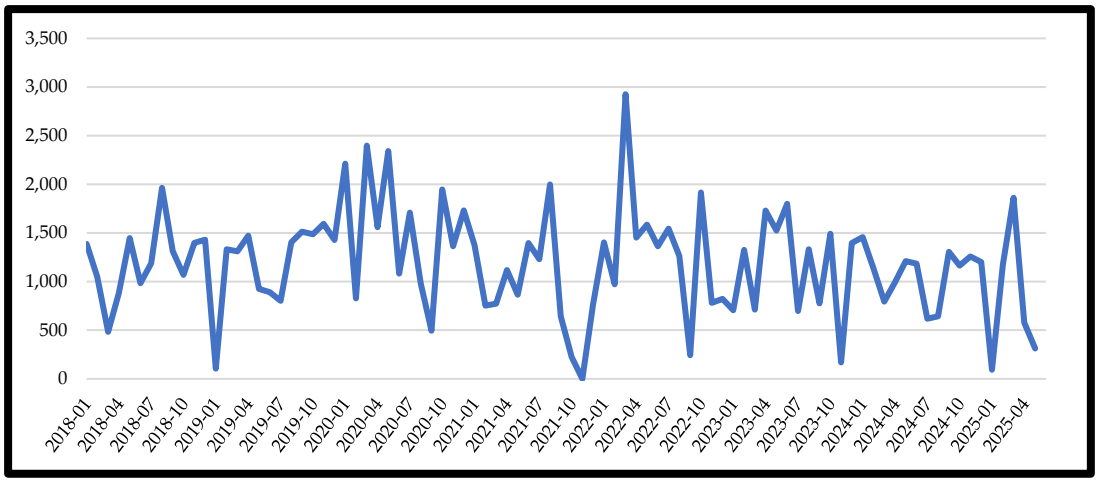
This threat vector remains active. As recently as August 2025, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and allied international partners confirmed that PRC state-sponsored actors continue to actively target global networks. According to the alert, these actors exploit "trusted connections to pivot into other networks" and compromise core router functions, including BGP routing.[118] These warnings establish the threat in principle. To measure it in practice, the Select Committee set out to quantify how often, and against whom, these carriers' networks have actually claimed American address space.

A. Large-Scale BGP Hijacking of American Networks

Focusing on the period January 1, 2018, through May 31, 2025, the Select Committee performed a multi-year assessment of global internet routing tables. Applying a rigorous, high-confidence detection methodology, the Select Committee identified 108,891 BGP hijack events in which PRC- or Hong Kong-associated carrier networks announced American internet address space without authorization.[119] This figure represents a conservative subset of the broader anomaly universe and excludes lower-confidence routing records that lacked sufficient corroboration. Although the dataset extends beyond the three U.S. subsidiaries specifically examined in this report, it shows that PRC- and Hong Kong-associated carrier ASNs repeatedly diverted U.S. traffic onto routing paths controlled by PRC state-owned or PRC-linked backbones.

This exposure affected at least 477 distinct U.S. networks—including premier telecommunications providers, Fortune 500 corporations, and critical infrastructure operators. More than 65,000 high-confidence events occurred between October 19, 2018, and mid-2025 with a substantial share happening after October 2022.[120]

Figure 6: BGP Hijack Event Timeline (January 2018 – May 2025)



Although the full dataset reflects a broader pattern of routing-security risks associated with PRC- and Hong Kong-linked telecommunications infrastructure, incidents involving the three state-owned carrier families examined in this report provide representative examples of how these vulnerabilities have affected U.S. networks in practice:

- A core communication network was the subject of at least nine unique hijack incidents attributable to China Mobile routing infrastructure.[121]

- One major telecommunications provider faced at least three unique hijack incidents originating from China Unicom routing claims.[122]

The corporate architecture of the U.S. subsidiaries substantially impeded after-the-fact forensic review by Select Committee investigators and shielded the parent network from accountability. Determining the exact nature of these massive routing spikes is fundamentally frustrated by limited visibility inside the domestic operations themselves. Testifying under oath when confronted with this routing data, Witness 4, a senior CTA engineering official, stated he had "no particular recollection" of the anomalies during this 16-day window and acknowledged that CTA's domestic NOC does not maintain traffic-flow logs.[123] By denying the domestic subsidiary basic logging capabilities, this structure left CTA personnel unable to explain the anomalies and left Select Committee investigators unable to reconstruct the relevant traffic flows, effectively shielding the parent network from accountability.

Given this forensic vacuum, the Select Committee does not contend that every one of these 108,891 routing events constitutes a deliberate, state-directed espionage operation. While some anomalies may indeed be the result of aggressive routing, configuration errors, or poor management, the underlying motive is secondary to the systemic risk. Regardless of whether these disruptions are intentional or accidental, the absence of local logging prevents accountability while facilitating a persistent pattern of unauthorized data diversion. This mechanism effectively forces American traffic into PRC-controlled infrastructure, providing Beijing with a permanent, unmonitored opportunity for passive surveillance.

Yet the companies displayed an unwillingness to acknowledge basic facts about the PRC's cyber operations. Despite extensive news coverage of what has been described as the largest telecom hack in history, witnesses from all three telecom companies denied awareness about the Typhoon campaigns.[124] Some claimed not even to be familiar with news reporting of PRC Government cyber intrusions generally. Even the most charitable interpretation – that employees of PRC state-controlled companies do not want to admit wrongdoing of the PRC Government on the record – is revealing in and of itself.

This activity cannot be stopped by FCC rulemaking alone. The routing manipulation documented here involved PRC and Hong Kong-associated carrier networks announcing American address space from positions outside ordinary U.S. licensing control. The FCC's pending rule can restrict domestic authorization and domestic interconnection with Covered List entities, but it cannot compel a foreign AS to withdraw an unauthorized route announcement made to networks abroad. Closing the routing-layer dimension of this threat requires allied network operators to enforce common route origin validation standards, share rapid route-leak notifications, and refuse to propagate unauthorized announcements from high-risk carriers.[125]

B. Case Studies of State-Sponsored Threats

While the preceding analysis established the scale of these routing anomalies, the following case studies identify the specific customers purchasing and operationalizing these commercial routing, transit, and data center services. In each instance below, Chinese state-controlled carriers sold underlying network access to entities tied directly to the PRC's defense and intelligence apparatus. These brokered relationships allowed hostile cyber actors to acquire the domestic routing cover, path continuity, and trusted peer status necessary to execute state-directed operations from within a legitimate American network footprint.

Case Study 1: China Telecom Americas and Qihoo 360

Technical data indicates that Qihoo 360 Technology Co., Ltd. (Qihoo 360) used CTA's network to maintain a trusted domestic routing path. During the September 2024 public disclosure of the Salt Typhoon intrusion, routing activity associated with Qihoo 360 and CTA surged in close synchronization.

Qihoo 360 is sanctioned by the U.S. government for its role in the CCP's military-civil fusion projects.[126] The company leads a dedicated innovation center tasked with building state-directed "cyber militia" units,[127] reflecting CEO Zhou Hongyi's doctrine that software vulnerabilities are a "national strategic resource."[128] That doctrine is also visible in Qihoo 360's role as one of only 29 "Tier 1" contributors to the CNNVD.[129] Leaked data from state cyber contractor i-SOON, as analyzed by private cybersecurity researchers, suggests that Qihoo 360-linked commercial antivirus customer telemetry may have been made available to government intelligence clients for target tracking.[130] Private cybersecurity researchers have also reported a possible Qihoo 360 link to the hack of a U.S. insurance company.[131]

Despite these national security concerns, global routing records confirm that Qihoo 360's AS55992 peers directly with CTA's AS36678.[132] Qihoo's domestic subsidiary, QIHU 360 Inc., also maintains active U.S.-registered IP addresses.[133] Through this peering relationship, CTA gave a designated Chinese military company a domestic interconnection path for routing traffic. That arrangement allowed Qihoo 360's traffic to move through routine commercial routing channels, rather than appearing only as traffic from a PRC-based network identity.

To evaluate how this relationship operated during a critical cyber incident, the Select Committee analyzed BGP routing updates in 15-minute increments from September 22 through 25, 2024, the four days immediately preceding *The Wall Street Journal*'s public disclosure of the Salt Typhoon intrusion into U.S. telecommunications systems.[134] Across 145 observation intervals, BGP announcement volumes for Qihoo 360 and CTA moved together in a statistically significant pattern.[135] In practical terms, their routing activity tended to rise and fall at the same time, rather than behaving like two unrelated commercial networks operating independently.

Other technical indicators point in the same direction. Scans of Qihoo 360's U.S.-announced IP addresses found active administrative and VPN-related systems, the types of internet-facing services that can support network management, software-update relays, control panels, or scanning activity.[136] Shodan data shows that many of these services went offline in August 2024, only weeks before Salt Typhoon became public.[137] That timing is consistent with Qihoo 360 hardening, hiding, or shutting down exposed infrastructure before the intrusion was publicly disclosed.

The Select Committee does not assert that this routing correlation proves CTA had subjective knowledge of, or deliberately participated in, any specific malicious payloads. The findings are structural. By maintaining an open peering relationship with a designated foreign military company, CTA provided a stable domestic routing path that allowed a high-risk PRC-linked entity to obscure its network footprint and reduce the technical friction needed to move traffic through U.S. infrastructure toward PRC-controlled networks.

Case Study 2: China Mobile and Salt Typhoon

Technical data from the Salt Typhoon cyber campaign reveals two distinct routing patterns involving CMI USA. The first pattern involves CMI USA infrastructure acting as a conduit that maintained internet paths to the hackers' servers. The second involves CMI USA networks simultaneously executing unauthorized routing changes that intercepted U.S. traffic. The Select Committee does not assert that CMI USA personnel had knowledge of, or participated in, these operations. These patterns do not definitively attribute the underlying cyber campaign to the company. However, the data demonstrates a highly concerning, dual-threat pattern of network behavior.

The first pattern highlights how CMI USA's network maintained internet paths to Salt Typhoon's infrastructure while U.S. defenders were actively attempting to remediate the intrusion. During the critical exposure window of September 22–25, 2024, the Select Committee tracked 58 internet prefixes linked to CISA-confirmed Salt Typhoon attacker servers.[138] Route checks conducted every eight hours revealed that China Mobile International's network (AS58453)—which is associated with relevant China Mobile USA routing—appeared in the active routing paths to those attacker servers at least 192 times. Consequently, even as U.S. defenders worked to sever the hackers' access, CMI USA's infrastructure

provided path continuity, keeping the attackers' operational backend accessible to the internet. This continuity coincided with severe operational compromises.

In November 2024, the FBI and CISA stated that PRC-affiliated actors had "compromised networks at multiple telecommunications companies" and enabled "the theft of customer call-records data," "the compromise of private communications" of certain government or political figures, and "the copying of certain information" subject to court-authorized U.S. law enforcement requests.[139] FBI Director Christopher Wray later described Salt Typhoon as potentially "the PRC's broadest, most significant cyber espionage campaign in history" that used access to telecommunications networks to target victims globally.[140]

The second pattern, drawn from the same master corpus of empirical data analyzed in the previous section, indicates that China Mobile networks were concurrently executing unauthorized routing changes on active U.S. internet traffic. Between January 1, 2018, and May 31, 2025, China Mobile-controlled networks (AS9808, AS56048, AS56040, and AS58453) were logged executing 4,213 high-confidence BGP anomalies or hijacks affecting or targeting American corporate networks.

Granular logs from this collective dataset confirm that the September 2024 Salt Typhoon exposure window intersected with a massive surge in global routing manipulation. During that exact month, PRC and Hong Kong-linked infrastructure initiated 1,305 separate high-confidence BGP hijacks against U.S. entities. China Mobile assets actively participated in this surge, executing 49 verified incidents. Notably, this included 8 high-severity hijacks directly originated by AS58453—the exact same network providing routing continuity to the attacker servers. These eight incidents forcibly misrouted and intercepted traffic belonging to targeted U.S. network operators. Taken together, this technical data reveals a highly concerning, dual-threat pattern of behavior.

Case Study 3: China Mobile USA and CloudRadium

Technical, testimonial, and subpoenaed documentary evidence indicates that China Mobile USA and CMI provided CloudRadium (HK) Limited (CloudRadium) access inside critical U.S. internet infrastructure that ordinary domestic suppliers were unwilling to directly provide. CloudRadium is a Hong Kong IP transit and hosting provider whose infrastructure repeatedly appeared in malicious cyber activity.[141]

In the United States, it operates through CloudRadium L.L.C. (CloudRadium), a Wyoming company formed in October 2012, and GlobalData Investments Inc., a California corporation that describes CeraNetworks as its brand and markets U.S. hosting, anti-DDoS, and data center services.[142]

Starting around 2014, CloudRadium turned to China Mobile USA and CMI for connectivity and data center access, relying on the PRC carrier to purchase space, power, and cross-connections from domestic suppliers that, according to Witness

1, were often "not willing to sign contracts directly" with new or unvetted customers.[143] By standing in as the contracting party, CMI supplied the commercial trust layer CloudRadium could not obtain on its own, much as CTA later provided Qihoo 360 a trusted domestic routing path.

Subpoenaed order forms confirm this arrangement in CMI's own documentation. Between January 2024 and May 2025, CloudRadium executed at least six orders with CMI listed as the seller of record.[144] Each form identified CMI as the buyer's agent, meaning CMI procured the services from third-party U.S. providers on CloudRadium's behalf.[145] In effect, CMI became the trusted counterparty that domestic vendors would not accept directly.

These orders gave CloudRadium access to two of the most sensitive internet interconnection sites in the United States.[146] All circuits were routed as CM-On-Net and the relationship expanded over time. Early 2024 orders provided 30 Gbps of guaranteed capacity, bursting up to 70 Gbps.[147] By May 2025, CloudRadium signed a 48-month contract valued at $480,000, which CMI billed together with its other U.S. circuits.[148] Internal CMI records described the setup as a coordinated U.S. buildout, with one circuit labeled as part of ten circuits in a U.S. expansion.[149] CMI countersigned the final order on May 27, 2025, well after the FCC's revocation of certain Chinese carrier authorizations.[150]

Internal records from both companies confirm they act as direct traffic partners, using multiple digital pathways—including those tied to CloudRadium—to keep their networks deeply and redundantly connected.[151]

During the May 2017 WannaCry ransomware outbreak, cybersecurity researcher Lee Neubecker used Shodan to identify internet addresses in the United States exposing the network service targeted by WannaCry. These searches measured internet exposure and potential attack surface. His May 15 query returned 42,973 results geolocated to Cheyenne, Wyoming. A separate May 17 nationwide query associated 42,746 of 499,402 United States results with CloudRadium, or 8.56 percent.[152] Neubecker subsequently reported that most of the Cheyenne results used IP addresses associated with CloudRadium.[153] CloudRadium's Wyoming corporate registration used an address near F.E. Warren Air Force Base, home to the 90th Missile Wing and its Minuteman III intercontinental ballistic missiles.

The United States attributed WannaCry to North Korea's Lazarus Group, a finding the Select Committee does not dispute.[154] A China nexus nonetheless runs through the operation's periphery. The Justice Department's charging documents placed part of the conspiracy's activity in China, and independent linguistic analysis of the ransom notes assessed with high confidence that their authors wrote fluently in Chinese, consistent with southern China, Hong Kong, Taiwan, or Singapore.[155] The FBI's investigation identified a broader operational infrastructure that included North Korea, Chinese, and other IP address, including addresses registered to China Unicom Liaoning.[156] These confirm a PRC linked component within the actors' border operating environment.

This same infrastructure repeatedly resurfaced. In 2018, researchers tracking WannaMine—a Monero-mining worm that spread through the same leaked NSA exploit WannaCry had weaponized—traced two of its command-and-control servers to CloudRadium.[157] They described a company with a disconnected phone number operating from a Los Angeles address shared with numerous other hosting and colocation providers, an address that also appears in CloudRadium-related corporate records.[158] In 2021, the United Kingdom's National Cyber Security Centre ranked CloudRadium among the ten largest hosts of fraudulent online shops worldwide, attributing 2,342 scam campaigns to its infrastructure.[159]

Case Study 4: China Unicom and Integrity Technology Group

Integrity Technology Group Inc. ("Integrity Tech"), a publicly traded Beijing-based cybersecurity firm, built its core business around cyber ranges, which are interactive simulated platforms that replicate networks, systems, and applications to mimic real-world environments, together with security testing and vulnerability research.[160] The firm's strategic value centers on KRLab, its research unit. KRLab markets attack-and-defense capabilities to commercial clients, and it also operates a "reconnaissance line" that supplies cybercrime intelligence collection to public security organs.[161] Those services align the firm's commercial catalog with the operational needs of the MSS and the PLA.[162]

The firm's turn toward state-aligned work followed a substantial injection of state-backed capital. In December 2020, a fund backed by state-owned capital led financing of roughly 200 million yuan (or about $30 million at the exchange rate of that period) after which Integrity Tech expanded the activities that would define its later profile.[163]

A joint advisory issued on September 18, 2024, by the FBI, the NSA, and the Cyber National Mission Force identified Integrity Tech infrastructure as the control layer for a botnet that had operated since mid-2021.[164] The botnet enrolled compromised Internet of Things devices to disguise malicious traffic, and it used China Unicom Beijing Province Network IP addresses both to manage the network and to reach other operational infrastructure deployed against U.S. victims.[165] A management application named "Sparrow," stored in a code repository that contained direct references to KRLab, served as the operational engine of the botnet.[166] As of June 2024, the network held more than 260,000 compromised devices, and its management database recorded over 1.2 million historical compromise records, including more than 385,000 unique U.S. victim devices.[167] In an unsealed search and seizure warrant, an FBI investigator assessed that the firm was "responsible, at least in part, for the computer intrusion activities collectively attributed to Flax Typhoon."[168f] The United States seized the command

[f] Flax Typhoon, Ethereal Panda, and RedJuliett are three designations used by U.S. cyber companies for the same cyber actor which falls under a broader CCP cyber campaign.

infrastructure in September 2024, and the Treasury Department sanctioned Integrity Tech on January 3, 2025, actions that together dismantled the operation.[169]

Integrity Tech infrastructure also supported a sustained espionage campaign against Taiwan. Beginning in 2023, reporting from CrowdStrike, Microsoft, and Recorded Future documented a group operating under the aliases Ethereal Panda and RedJuliett that targeted Taiwanese government, aerospace, and critical-technology organizations, with particular attention to entities tied to the military.[170] Recorded Future's Insikt Group geolocated suspected administrative activity to Fuzhou, Fujian, PRC, and assessed that the group likely operates from that city.[171] Integrity Tech maintains an office in the Fuzhou Software Park, and analysts have identified that geographic overlap as one factor supporting a possible connection between the firm's state-funded research and the tradecraft directed at these targets.[172]

The firm's proximity to the MSS surfaced again one week before the September 2024 advisory. Integrity Tech and "China Unicom"[g] served as lead editors, together with the China Information Technology Security Evaluation Center ("CNITSEC"), on a white paper that set out the same category of vulnerability-testing tradecraft later identified in the botnet investigation.[173] Testimony before the U.S.-China Economic and Security Review Commission described CNITSEC as functioning as a public-facing cover for the 13th Bureau of the MSS.[174]

China Unicom's relationship with Integrity Tech reaches well beyond the botnet infrastructure. In November 2023, while the botnet remained active, the two companies formalized a "comprehensive strategic cooperation" for a "co-chain ecosystem cooperation agreement."[175] The arrangement produced a steady stream of government-backed work. China Unicom's Software Research Institute repeatedly selected Integrity Tech to build attack-and-defense training platforms and to run security competitions, frequently through sole-source awards for red-team and blue-team exercises.[176] By 2025 the relationship had widened, and Unicom moved to integrate Integrity Tech into its core security operations and its work on AI-driven defense.[177] A firm that the United States had identified as a conduit for attacks on American critical infrastructure now sat inside the offensive-training apparatus of one of China's largest state-owned carriers.

Integrity Technology is not the only cybersecurity contractor associated with China Unicom's broader security ecosystem. China Unicom also appeared as a corporate partner of i-SOON, a Shanghai contractor whose primary customers were PRC government agencies, including the MSS and the Ministry of Public Security ("MPS").[178] Prosecutors in the Southern District of New York alleged that i-SOON worked with at least 43 different MSS or MPS bureaus and charged

[g] The public facing announcements in Mandarin do not delineate anything more than "China Unicom."

between roughly $10,000 and $75,000 for each email inbox it successfully compromised.[179] Two of China Unicom's cybersecurity partners therefore sit among the recognized commercial pillars of the state's hacking-for-hire ecosystem.

The provincial architecture of Chinese state security helps explain how a Beijing carrier connects to this network of contractors and government customers. China Unicom's Beijing network falls within the remit of the Beijing State Security Bureau, a provincial-level intelligence and counterintelligence organ subordinate both to the MSS and to Beijing's municipal leadership. Official U.S. attributions provide concrete examples. The Department of Justice has attributed APT40 to the Hainan State Security Department and APT10 to the Tianjin State Security Bureau.[180]

China Unicom has also invested in cybersecurity capability of its own. It built much of that capability in-house, through China Unicom Digital Technology and the Software Research Institute. In September 2025, the cybersecurity large language model produced by China Unicom Digital Technology was selected for Beijing's 2025 catalog of major first-of-their-kind technical equipment. The company presented itself as China's national cybersecurity team and emphasized applications in security operations, attack-and-defense, and the protection of critical information infrastructure.[181]

China Unicom appears throughout this case study in multiple capacities. Its network infrastructure supported the botnet described by U.S. authorities. Its parent company co-edited cybersecurity research with organizations publicly associated with the MSS. Its procurement arm continued awarding cybersecurity work to Integrity Tech after U.S. sanctions. Its digital technology subsidiary simultaneously expanded an in-house offensive and defensive cybersecurity capability. Taken together, these documented activities illustrate that China Unicom functions as more than a traditional telecommunications carrier. It operates as an integrated participant within China's broader state cybersecurity ecosystem.

Recommendations

Between 2019 and 2022, the FCC took major national security actions against CMI USA, CTA, and CUA under Section 214 of the Communications Act. The Commission denied China Mobile USA's application for international Section 214 authority and later revoked or terminated the Section 214 authorizations of China Telecom Americas and China Unicom Americas after finding that their continued operations presented national security and law-enforcement risks.[182] The Commission has since moved to address a related domestic gap. On April 30, 2026, the FCC adopted a Notice of Proposed Rulemaking proposing to exclude Covered List entities from the blanket Section 214 authority that most domestic carriers have received automatically since 1999 and seeking comment on further exclusions beyond the Covered List. The Section 214 revocations and denials between 2019 and 2022 were important milestones, and the new 2026 proceeding is directionally correct. The Select Committee commends past and present Commissions for pursuing this work.

These actions restrict the companies' ability to provide covered telecommunications services in the United States, but under current law they did not create a complete infrastructure-removal remedy. Nor, by itself, would the pending blanket-authority rulemaking fully solve the problem identified in this report. Section 214 is a licensing tool. It does not require a foreign state-controlled carrier or its affiliates to remove retained Points of Presence, colocation equipment, cross-connects, peering relationships, IP transit arrangements, parent-controlled ASNs, or remote network operations that may persist outside the licensed service. Existing tools, including the FCC Covered List, Team Telecom review, Commerce's ICTS program, and CISA, NSA, and FBI hardening guidance, address important parts of the risk, but they do not fully close the gap between telecommunications licensing and modern internet infrastructure.[183] Legitimate infrastructure needed to facilitate the flow of internet traffic between the U.S. and China is useful, but it need not be controlled by PRC entities on U.S. soil where it can be subverted for illegitimate purposes that threaten our national security.

Longstanding bipartisan action against the three PRC state-controlled telecom companies and the FCC's pending NPRM validate the core premise of this report. The latter would address the licensing issue by excluding Covered List entities from blanket domestic Section 214 authority. It addresses part of the trusted connection problem by seeking comment on prohibiting telecommunications carriers from interconnecting with excluded or revoked entities, including through facilities such as Points of Presence and data centers. The proposed rule also explores whether holders of Covered Authorizations[h] should be restricted from transactions or other dealings with high-risk entities and whether unlicensed wireless rules should be modified to prevent a comparable end run. But the NPRM

[h] See Foreign Adversary Control Report and Order, FCC 26-2, at *44, Appx. A (§ 1.80001) ("The term Covered Authorization means a license, lease, authorization, permit, grant, or other approval granted by the Commission that appears on a Schedule as described in § 1.80002.")

operates through the authorities available to the Commission. It does not create a separate statutory retained infrastructure regime. That framework would need to define the covered infrastructure, assign review authority, require interim monitoring, fund removal or mitigation, address private unlicensed network arrangements, and support international routing security enforcement. The rulemaking is confirmation of the threat and is a key first step. Congress should now codify the protection, expanding it beyond current licensing regulations and authorities, and fund the tools required to remove or mitigate the retained infrastructure this report documents.

To close that gap, the Select Committee recommends that Congress build on prior actions, including proposed rules, and enact targeted legislative and appropriations measures to identify, restrict, mitigate, and where necessary remove foreign state-controlled network infrastructure that presents a continuing national security risk.[184]

1. **Codify the FCC's authority to deny blanket authorizations and domestic interconnection.** Congress should codify the FCC's authority to exclude Covered List entities, and other entities subject to the jurisdiction or control of a foreign adversary, from operating under blanket Section 214 authority. Congress should also prohibit domestic telecommunications carriers from interconnecting with Covered List entities absent affirmative FCC authorization following executive branch national security review. Any final rule should reach PoPs, data centers, colocation facilities, cross-connects, IP transit, private peering, and routing arrangements that preserve operational access to U.S. communications infrastructure.

2. **Establish statutory authority over retained foreign-adversary infrastructure.** Congress should authorize the FCC, Team Telecom, and Commerce's ICTS program to identify, restrict, mitigate, and where necessary remove foreign adversary-connected physical and logical network infrastructure that remains in the United States after license denial, license revocation, Covered List designation, or an evidence-based national security finding.

3. **Broaden Team Telecom and ICTS jurisdiction over private commercial arrangements.** Congress should authorize Team Telecom and Commerce's ICTS program to review private, unlicensed commercial arrangements involving foreign adversary-controlled internet infrastructure, including private colocation agreements, unregulated IP transit contracts, enterprise network service purchases, and parent-controlled remote operations that may not require an FCC license. Congress should require disclosure and risk review of material network-service relationships between major domestic technology companies and Covered List entities.

4. **Mandate entity-specific Covered List determinations and fund targeted "rip-and-replace."** Congress should require the FCC, Commerce, and relevant national security agencies to complete entity-specific Covered List determinations for high-risk manufacturers and service providers identified in congressional or agency records. Concurrently, Congress should appropriate targeted removal funding for the highest-risk deployments in sensitive telecommunications, energy, and defense industrial base networks, with replacement obligations made contingent on available appropriations.

5. **Fund multilateral routing-security enforcement and ensure federal agencies have the talent they need to address PRC cyber threats.** Congress should appropriate or use dedicated funding, such as the Cyberspace, Digital Connectivity, and Related Technologies Fund, for the Department of State and CISA to build allied commitments around baseline BGP routing security standards, route-origin validation, rapid route-leak notifications, and coordinated refusal to propagate unauthorized announcements from high-risk carriers. This fills the gap that domestic FCC rules cannot reach: routing conduct by foreign autonomous systems outside U.S. jurisdiction. To fulfill this critical mission, Congress should also ensure U.S. cybersecurity agencies have the funding, resources, and talent they need to protect our security and coordinate with our allies.

6. **Require interim logging and monitoring pending removal or mitigation.** Congress should require minimum logging, monitoring, and record-preservation obligations for any foreign adversary-connected entity that retains U.S. network infrastructure, colocation space, routing identities, or parent-controlled network operations access pending removal, mitigation, or wind-down. These obligations should apply regardless of whether the entity still holds an FCC license and should preserve records sufficient for designated national security agencies to conduct retrospective routing-forensics analysis.

Classified Annex

A classified annex is on file with the Committee. Parties with appropriate access can reach out to the Committee for inquiries.

[1] Worldwide Threats to the Homeland, Statement Before the U.S. House Committee on Homeland Security, Michael Glasheen, Federal Bureau of Investigation, December 11, 2025, https://www.fbi.gov/news/speeches-and-testimony/worldwide-threats-to-the-homeland-121125.
[2] Section 214 of the Communications Act (47 U.S.C. § 214) requires a carrier to obtain FCC authority before constructing, acquiring, operating, or engaging in transmission through certain communications lines where the public convenience and necessity require such authority. Domestic blanket authority historically allowed qualifying domestic carriers to operate without individualized application.
[3] A Point of Presence is a physical location, often a rack or cage in a data center, where a network operator maintains equipment and network connections. PoPs allow a carrier to extend its network into a geographic market and exchange traffic with other networks at that site.
[4] China Mobile Int'l (USA) Inc., 34 FCC Rcd 3361 (2019); China Telecom (Ams.) Corp., 36 FCC Rcd 15966, 16008, para. 65 (2021); China Unicom (Ams.) Operations Ltd., 37 FCC Rcd 1480, 1530, para. 74 (2022).
[5] Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure (Nov. 13, 2024), https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications.
[6] Cybersecurity & Infrastructure Sec. Agency et al., Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System, Alert No. AA25-239A (Aug. 27, 2025, rev. Sept. 3, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a; Nat'l Sec. Agency, NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations (Aug. 27, 2025), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/.
[7] End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses: Hearing Before the H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, 119th Cong. (Mar. 5, 2025), https://chinaselectcommittee.house.gov.
[8] Letters from Chairman John Moolenaar and Ranking Member Raja Krishnamoorthi to China Mobile International Ltd., China Telecom (Ams.) Corp., and China Unicom (Ams.) Operations Ltd. (Mar. 3, 2025).
[9] Michael Martina, *US Lawmakers Subpoena China Telecom Giants Over Security Concerns*, Reuters (Apr. 23, 2025, 4:24 PM), https://www.reuters.com/sustainability/boards-policy-regulation/us-lawmakers-subpoena-china-telecom-giants-over-security-concerns-2025-04-23/.
[10] Subpoenas from H. Select Comm. to China Mobile International Ltd., China Telecom (Ams.) Corp., and China Unicom (Ams.) Operations Ltd. (Apr. 23, 2025).
[11] Liu Caiyu, US lawmakers' subpoena of Chinese telecom firms over security concerns a clear case of political manipulation: expert (2025); https://www.globaltimes.cn/page/202504/1332811.shtml.
[12] BGP routing records, documents on file with the Committee,
[13] Cybersecurity and Infrastructure Security Agency, U.S. Dep't of Homeland Security (on file with the Committee).
[14] Cloudflare, BGP Hijack Database, https://radar.cloudflare.com/routing.
[15] Shodan, https://www.shodan.io; Censys, https://censys.io, scan June 2025.
[16] *See* China Mobile Int'l (USA) Inc., Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019); China Telecom (Americas) Corp., Order on Revocation and Termination, 36 FCC Rcd 15966 (2021); China Unicom (Americas) Operations Ltd., Order on Revocation, 37 FCC Rcd 1480 (2022); *see also* China Unicom (Americas) Operations Ltd., Order to Show Cause, 35 FCC Rcd 3713 (IB/WCB/EB 2020).
[17] SASAC supervises and administers the State Council's ownership interests in China's central state-owned enterprises. *See* China Mobile Int'l (USA) Inc., 34 FCC Rcd at 3363–64, paras. 3, 8.
[18] China Unicom (Americas) Operations Ltd., Order to Show Cause, 35 FCC Rcd. 3716, 3721, 3723 n.16 (citing Edge Cable Holdings USA, LLC, et al., Application for a License to Land and Operate a Private Fiber-Optic Submarine Cable System, File No. SCL-LIC-20180711-00018, Attach. 1, Appx. D at 1–2 (filed July 11, 2018)).
[19] Transcribed Interview of Witness #5, at pp. 19 and 21 (Sept. 10, 2025).
[20] U.S. Dep't of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense

Authorization Act for Fiscal Year 2021 (June 8, 2026), https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF. DoD renders the China Telecom parent as "China Telecom Group Co., Ltd.," however, the company's annual filings and Treasury's NS-CMIC List render the same entity (中国电信集团有限公司) as "China Telecommunications Corporation." *See* China Telecom Corp. Ltd., Annual Report 2025, at 3 (2026), https://www.chinatelecom-h.com/en/ir/report/annual2025.pdf.

[21] Off. of Foreign Assets Control, U.S. Dep't of the Treasury, Non-SDN Chinese Military-Industrial Complex Companies List, https://www.treasury.gov/ofac/downloads/ccmc/nscmiclist.pdf; *see* Exec. Order No. 14,032, 86 Fed. Reg. 30,145 (June 7, 2021); 31 C.F.R. pt. 586.

[22] National Intelligence Law of the People's Republic of China [国家情报法] arts. 7, 14 (effective June 27, 2017); see also Data Security Law of the People's Republic of China [数据安全法] (effective Sept. 1, 2021).

[23] China Unicom (Americas), Responses to Subpoena from the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (May 9, 2025), p. 3.

[24]Transcribed Interview of Witness # 5, at pp.84-86 and 89-90 (Sept. 10, 2025).

[25] Transcribed Interview of Witness # 6, at pp.20-24 (Sept. 11, 2025) and Transcribed Interview of Witness #7 at pp. 19-20.

[26] Transcribed Interview of Witness # 5, at p. 14 (Sept. 10, 2025).

[27] Transcribed Interview of Witness # 5, at p. 14 (Sept. 10, 2025) and Transcribed Interview of Witness #5 at pp. 8-10 and 33-36.

[28]Transcribed Interview of Witness # 5, at p. 15 (Sept. 10, 2025).

[29] Transcribed Interview of Witness # 5, at pp. 43-44 (Sept. 10, 2025).

[30] Transcribed Interview of Witness # 5, at p. 53 (Sept. 10, 2025).

[31] Transcribed Interview of Witness #5, at p. 44 (Sept. 10, 2025).

[32] *Id*. at p. 45.

[33] Transcribed Interview of Witness # 3, at p. 17, p. 29 (Sept. 29, 2025).

[34] Transcribed Interview of Witness # 3, at pp. 43-44 (Sept. 29, 2025).

[35] Transcribed Interview of Witness # 4, at p. 14 (Sept. 29, 2025).

[36] Transcribed Interview of Witness # 4, at pp. 24-25 (Sept. 29, 2025).

[37] Transcribed Interview of Witness # 3, at p. 39 (Sept. 29, 2025).

[38] Transcribed Interview of Witness # 1, at p. 22 (Sept. 17, 2025).

[39] Federal Communications Commission, China Mobile International (USA) Inc., Application for Global Facilities Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, Memorandum Opinion and Order, 34 FCC Rcd. 3361, ¶¶ 14, 30 to 33 (2019), https://docs.fcc.gov/public/attachments/FCC-19-38A1.pdf (finding that China Mobile USA was ultimately owned and controlled by the People's Republic of China through the China Mobile corporate structure, concluding that the company was vulnerable to exploitation, influence, and control by the Chinese government, and determining that granting international Section 214 authority would pose substantial national security and law enforcement risks despite the absence of public evidence that China Mobile USA had previously been used for espionage activities).

[40] Transcribed Interview of Witness # 2, at p. 2 (Sept. 17, 2025).

[41] Transcribed Interview of Witness # 1, at p. 23 (Sept. 17, 2025).

[42] Transcribed Interview of Witness # 1, at p. 26 (Sept. 17, 2025).

[43] 47 U.S.C. § 214(a).

[44] China Telecom (Americas) Corp., Order on Revocation and Termination, 36 FCC Rcd. 15966, ¶ 157 (2021). See also Press Release, FCC, *FCC Revokes and Terminates China Telecom America's Authority to Provide Telecom Services in America* (Oct. 26, 2021), https://docs.fcc.gov/public/attachments/DOC-376902A1.pdf.

[45] *Protecting Against National Security Threats in Domestic Telecommunications Service*, Notice of Proposed Rulemaking, 91 Fed. Reg. 25327, 25329–30 (May 8, 2026), https://www.federalregister.gov/documents/2026/05/08/2026-09190/protecting-against-national-security-threats-in-domestic-telecommunications-service.

[46] *Id*.

[47]See 47 U.S.C. sec. 214(a); In re China Telecom (Americas) Corp., Order on Revocation, FCC 21-114, 36 FCC Rcd 15966 (2021); In re China Mobile Int'l (USA) Inc., Memorandum Opinion and Order, FCC

19-38, 34 FCC Rcd 3361 (2019); In re China Unicom (Americas) Operations Ltd., Order on Revocation, FCC 22-9, 37 FCC Rcd 978 (2022).

[48] Letter from Morgan, Lewis & Bockius LLP, to Hon. John Moolenaar, Chairman, and Hon. Raja Krishnamoorthi, Ranking Member, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, at 10 (May 28, 2025).

[49] Letter from Morgan, Lewis & Bockius LLP, to Hon. John Moolenaar, Chairman, and Hon. Raja Krishnamoorthi, Ranking Member, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, at 11 (May 28, 2025). Also, *see* CTA-SCCCP-000454 to CTA-SCCCP-000994.

[50] CTA-SCCCP-000770 to CTA-SCCCP-000801; CTA-SCCCP-000818 to CTA-SCCCP-000833; CTA-SCCCP-000980 to CTA-SCCCP-000994; CTA-SCCCP-001019 to CTA-SCCCP-001035; CTA-SCCCP-000697 to CTA-SCCCP-000708; CTA-SCCCP-000454 to CTA-SCCCP-000469; CTA-SCCCP-000470 to CTA-SCCCP-000487; CTA-SCCCP-000488 to CTA-SCCCP-000503; CTA-SCCCP-000504 to CTA-SCCCP-000520; CTA-SCCCP-000521 to CTA-SCCCP-000536; CTA-SCCCP-000537 to CTA-SCCCP-000552; CTA-SCCCP-000553 to CTA-SCCCP-000568; CTA-SCCCP-000608 to CTA-SCCCP-000618; CTA-SCCCP-000619 to CTA-SCCCP-000632; CTA-SCCCP-000649 to CTA-SCCCP-000664; CTA-SCCCP-000665 to CTA-SCCCP-000680; CTA-SCCCP-000681 to CTA-SCCCP-000696; CTA-SCCCP-000709 to CTA-SCCCP-000724; CTA-SCCCP-000757 to CTA-SCCCP-000769; CTA-SCCCP-000802 to CTA-SCCCP-000817; CTA-SCCCP-000834 to CTA-SCCCP-000850; CTA-SCCCP-000851 to CTA-SCCCP-000868; CTA-SCCCP-000869 to CTA-SCCCP-000884; CTA-SCCCP-000885 to CTA-SCCCP-000900; CTA-SCCCP-000901 to CTA-SCCCP-000917; CTA-SCCCP-000918 to CTA-SCCCP-000933; CTA-SCCCP-000934 to CTA-SCCCP-000945; CTA-SCCCP-000946 to CTA-SCCCP-000963; CTA-SCCCP-000964 to CTA-SCCCP-000979.

[51] CTA-SCCCP-000306 to CTA-SCCCP-000310; CTA-SCCCP-000323 to CTA-SCCCP-000395; CTA-SCCCP-000139 to CTA-SCCCP-000145; CTA-SCCCP-000146 to CTA-SCCCP-000195; CTA-SCCCP-000196 to CTA-SCCCP-000200; CTA-SCCCP-000396 to CTA-SCCCP-000429; CTA-SCCCP-000430 to CTA-SCCCP-000446; CTA-SCCCP-000447 to CTA-SCCCP-000453.

[52] Master Service Agreement between China Telecommunications Corporation and China Telecom (Americas) Corporation at CTA-SCCCP-000123 (Jan. 1, 2007).

[53] Master Services Agreement between China Telecom (Americas) Corporation and China Telecom Corporation Limited, Global Business Department at CTA-SCCCP-000118 (Apr. 1, 2016).

[54] International Ethernet Private Line Leased Circuit Order Form, CUA_HRCOMMCCP_0000762–64; China Unicom Internet Access Order Form for Singapore and Tokyo 4×100G Upgrade and New Pricing Model, CUA_HRCOMMCCP_0000752–61; Service Order for IP Paid Peering Services, CUA_HRCOMMCCP_0000747–51.

[55] China Unicom Internet Access Order Form for Singapore and Tokyo 4×100G Upgrade and New Pricing Model, CUA_HRCOMMCCP_0000752–61; Service Order for IP Paid Peering Services, CUA_HRCOMMCCP_0000747–51.

[56] Dedicated Internet Access Order Form and Acceptable Use Policy, CUA_HRCOMMCCP_0000765–70.

[57] Letter from Squire Patton Boggs (US) LLP to General Counsels, H. Select Comm. on the CCP, at 13 (July 13, 2025).

[58] CMIUSA000027_CONFIDENTIAL, CMIUSA-EB-002903

[59] CMIUSA-EB-002903 (IP Transit customers).

[60] China Mobile Int'l (USA) Inc., Services by Customer (FCC LOI Ex. 8), CMIUSA-EB-002903 (China Mobile Guangdong—IDC Resale, 9/9/2020–present). Customer Order Records, CMIUSA000027: China Mobile Communications Group Guangdong Co., Ltd., Shenzhen Branch (中国移动通信集团广东有限公司深圳分公司); China Mobile Communications Group Guangdong Co., Ltd., Guangzhou Branch (中国移动通信集团广东有限公司广州分公司); China Mobile Tietong Co., Ltd., Guangzhou Branch (中移铁通有限公司广州分公司) (CMIUSA000177_CONFIDENTIAL, CMIUSA000178_CONFIDENTIAL, CMIUSA000179_CONFIDENTIAL).

[61] Letter from Squire Patton Boggs (US) LLP to General Counsels, House Select Committee on the Chinese Communist Party at 10 (July 10, 2026). Also, *see* Letter from Harris, Wiltshire & Grannis LLP to U.S. Dep't of Commerce 4 (Apr. 1, 2021), CMIUSA_Commerce_000013 (Resp. to Req. 1.g–h); see also CMIUSA000227–CMIUSA000623.

[62] Letter from Squire Patton Boggs (US) LLP to General Counsels, House Select Committee on the Chinese Communist Party at 10 (July 10, 2026). Also, *see* CMIUSA_HC_0000458–62, China Mobile International Purchase Order, CMI Reference No. USS-PO-20210-00679; CMIUSA_HC_0000699–700,

China Mobile International Purchase Order, CMI Reference No. CMI-Q-CTS-202503552-ECCOM; CMIUSA_HC_0000715–17, China Mobile International Purchase Order, CMI Reference No. CMI-Q-CTS-202504553-ECCOM.

[63] Letter from Squire Patton Boggs (US) LLP to General Counsels, House Select Committee on the Chinese Communist Party at 10 (July 10, 2026). Also, *see* CMIUSA_HC_0000458–62, China Mobile International Purchase Order, CMI Reference No. USS-PO-20210-00679; CMIUSA_HC_0000699–700, China Mobile International Purchase Order, CMI Reference No. CMI-Q-CTS-202503552-ECCOM; CMIUSA_HC_0000715–17, China Mobile International Purchase Order, CMI Reference No. CMI-Q-CTS-202504553-ECCOM.

[64] ECCOM established ECCOM USA on September 7, 2010, through a wholly owned Hong Kong holding company, a structure disclosed in a 2012 restructuring report filed with the Shanghai Stock Exchange. California corporate records verify this incorporation and confirm that the Santa Clara-based entity engages in the "[s]ales and [s]ervice of IT" equipment. ECCOM's website even lists ECCOM USA among its operations in "Other Regions." Furthermore, ECCOM USA shares key personnel with ECCOM and its parent company, CETC Digital. Specifically, shared personnel include CFO Jianping Chen, who serves concurrently as vice general manager and CFO of CETC Digital; director Shimin Song, who held 17.5 percent of ECCOM before the 2012 share-issuance acquisition and remains a top ten shareholder of CETC Digital; and director Hong Zhang, who serves as ECCOM's executive president and sits on the board of CETC Digital. *See* Shanghai East-China Computer Co., Ltd. [上海华东电脑股份有限公司], *Report on the Purchase of Assets Through Share Issuance and Related-Party Transaction (Revised Draft) (Summary)* [发行股份购买资产暨关联交易报告书（修订稿）（摘要）] 29–30, 47–48 (June 2012), https://perma.cc/PVK5-4VGG; CETC Digital Technology Co., Ltd. [中电科数字技术股份有限公司], *2024 Annual Report* [2024年年度报告] 4, 24–25, 32–33, 66, 68–69 (Apr. 2025), https://www.shecc.com/Files/202504/16/9b9b269f-6959-4544-b9be-41a0c5e463f1.pdf; ECCOM Network (USA), Inc., Articles of Incorporation, Entity No. 3316762 (Cal. Sec'y of State filed Sept. 7, 2010); ECCOM Network (USA), Inc., Statement of Information, File No. BA20241440550, Entity No. 3316762 (Cal. Sec'y of State filed Aug. 7, 2024); ECCOM Network (USA), Inc., Statement of Information, File No. BA20251329036, Entity No. 3316762 (Cal. Sec'y of State filed June 22, 2025); *Other Regions* [其他地区], ECCOM Network System Co., Ltd. [上海华讯网络系统有限公司], https://perma.cc/XQJ2-QT3Z.

[65] *Non-SDN Chinese Military-Industrial Complex Companies List*, Off. of Foreign Assets Control, U.S. Dep't of the Treasury (entry for China Electronics Technology Group Corporation, effective Aug. 2, 2021), https://ofac.treasury.gov/consolidated-sanctions-list/ns-cmic-list; *Notice of Availability of Designation of Chinese Military Companies*, 90 Fed. Reg. 1,105, 1,105 (Jan. 7, 2025); U.S. Dep't of Def., *Entities Identified as Chinese Military Companies Operating in the United States* 3 (Jan. 7, 2025), https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF.

[66] China Telecom (Americas) Corporation, Further Responses to Subpoena the House Select Committee on the Strategic Competition Between United States and the Chinese Communist Party, at 3-4 (2025).

[67] *Id*. at 3.

[68] Transcribed Interview of Witness # 6 (Sept. 11, 2025); Transcribed Interview of Witness # 7 (Sept. 11, 2025).

[69] CUA_HRCOMMCCP_0000017–21, 54–56, 193–201, 244–326; CUA_HRCOMMCCP_0000064–70; 191–92; CUA_HRCOMMCCP_0000071–90, 210–21, 388–95; CUA_HRCOMMCCP_0000237–43; CUA_HRCOMMCCP_0000412–22; CUA_HRCOMMCCP_0000467–79; CUA_HRCOMMCCP_0000276.

[70] CUA_HRCOMMCCP_0000105–09, 227–30; CUA_HRCOMMCCP_0000110–167, 189–90, 396–411; CUA_HRCOMMCCP_0000022–53; CUA_HRCOMMCCP_0000091–98; CUA_HRCOMMCCP_0000099–104; CUA_HRCOMMCCP_0000327–87.

[71] China Mobile International (USA) Inc., Memorandum Opinion and Order, FCC 19-38, ¶ 8 (May 10, 2019) ("Thus, we deny China Mobile USA's application for international section 214 authority."); Letter from Squire Patton Boggs LLP, to General Counsels, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, at 8 (July 13, 2025).

[72] CMIUSA000624_CONFIDENTIAL, CMIUSA000625_CONFIDENTIAL.

[73] *Id*.

[74] *Id*.

[75] Select Committee Shodan scan of China Mobile network assets, conducted June 2025 (on file with Comm.).
[76] Joint Build Agreement, Bay to Bay Express Cable System §§ 1.1 ("Segment L"), sched. 3 (Fiber Pair Allocation), sched. 4 (Participation Interests) (2018) (CMIUSA000006–000008); see Application of Edge Cable Holdings USA, LLC, China Mobile Int'l Ltd. & Vadata, Inc. for a Cable Landing License, File No. SCL-LIC-20181125-00037 (FCC filed Nov. 25, 2018). Amid the U.S. government's campaign to block direct undersea connections between the United States and Hong Kong, the consortium withdrew its FCC cable landing license application on September 10, 2020, and the system was reconfigured as the U.S.–Philippines CAP-1 cable. On August 8, 2021, CMI agreed to transfer all of its rights, title, and interests in the Grover Beach facilities to Meta and Amazon and was removed as an applicant the following day, ending China Mobile's bid to own a cable terminating on American soil.
[77] The Hong Kong–Americas (HKA) consortium comprised Meta, China Telecom, China Unicom, RTI Express, Tata Communications, and Telstra. China Telecom and China Unicom each owned one fiber pair on the main trunk. The applicants withdrew the cable landing license application in March 2021 "due to ongoing concerns from the US government about direct communications links between the United States and Hong Kong." See Notice of Withdrawal of Cable Landing License Application, File No. SCL-LIC-20180711-00018 (FCC filed Mar. 9, 2021).
[78] *Id*.
[79] *See*, e.g., Pacific Light Cable Network, File No. SCL-LIC-20170421-00012; FCC 24-119, ¶¶ 82–83 (2024).
[80] Nicole T. Carter et al., Cong. Rsch. Serv., R47648, Protection of the Undersea Telecommunication Cables: Issues for Congress (2023), https://www.congress.gov/crs-product/R47648?__cf_chl_f_tk=YSSmw13jxwtRRCtJ8QyjryNCyhCDDNsE4P.2lJq8_5A-1782792178-1.0.1.1-wZ3iD30747Y4375AMtrT7kUKTpkJak57BMbE7pC4Ffw.
[81] U.S. Gov't Accountability Off., GAO-22-104560, Cybersecurity: Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks (Mar. 2022), https://www.gao.gov/assets/720/719340.pdf; Andrei Robachevsky et al, The Danger of the New Internet Choke Points, Internet Soc'y (Feb. 2014), https://www.internetsociety.org/wp-content/uploads/2017/08/The20Danger20of20the20New20Internet20Choke20Points_0.pdf.
[82] Letter from Morgan, Lewis & Bockius LLP, to Hon. John Moolenaar, Chairman, and Hon. Raja Krishnamoorthi, Ranking Member, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, at 4-8 (May 28, 2025).
[83] Letter from Morgan, Lewis & Bockius LLP, to Hon. John Moolenaar, Chairman, and Hon. Raja Krishnamoorthi, Ranking Member, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party, at 6 (May 28, 2025).
[84] Transcribed Interview of Witness # 4, at p. 13 (Sept. 29, 2025).
[85] *Id.;* Committee Shodan Scan, June 2025.
[86] For China Mobile, https://www.ruijie.com/en-global/about/news/75086; For China Telecom and China Unicom, https://www.ruijie.com/en-global/about/news/76261.
[87] China Nat'l Vulnerability Database of Info. Sec. [国家信息安全漏洞库], Technical Support Units [技术支撑单位], https://perma.cc/2VHF-YJY4.
[88] Recorded Future, *China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers Over Foreign Technology* (Aug. 31, 2017), https://www.recordedfuture.com/china-cybersecurity-law/.
[89] The equipment manufacturer discussed here, Ruijie Networks Co., Ltd. of Fuzhou, is a separate entity from Sichuan Zhixin Ruijie Network Technology Co., Ltd., a Chengdu-based firm founded in 2018. The latter was named in CISA Joint Cybersecurity Advisory AA25-239A as one of three Chinese companies that supply cyber-related products and services to units of the Ministry of State Security and the People's Liberation Army in support of the Salt Typhoon campaign. Ruijie Networks' authorized distributor has stated that the manufacturer has no relationship with that firm. The Select Committee does not treat the two as related in this report based on publicly available information. *See* Cybersecurity & Infrastructure Sec. Agency et al., Joint Cybersecurity Advisory AA25-239A, *Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System* (Aug. 27, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a; Visiotech, *Clarification Statement on Ruijie Networks' Non-Involvement in Cyber-Espionage Allegations* (Sept. 17, 2025), https://www.visiotechsecurity.com/en/news/396-clarification-statement-on-ruijie-networks-non-involvement-in-cyber-espionage-allegations-against-chinese-companies.

[90] Staff Analysis of Shodan and Censys Network Scan Data for Ruijie Associated Devices in U.S. Networks, (on file with the Select Committee), June 2025.
[91] Cybersecurity & Infrastructure Sec. Agency, ICS Advisory ICSA-24-338-01, *Ruijie Reyee OS* (Dec. 10, 2024), https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-01.
[92] Protecting Against National Security Threats in Domestic Telecommunications Service, Notice of Proposed Rulemaking, WC Docket No. 26-82, FCC 26-29, paras. 7-8, 11-18, 19-22 (rel. May 1, 2026), published at 91 Fed. Reg. 25325, (May 8, 2026). paras. 13-16 (tentatively concluding that national security concerns support limits on interconnection with Covered List entities and seeking comment on prohibitions involving facilities including Points of Presence and data centers, existing agreements, transition periods, and possible retroactive application), https://docs.fcc.gov/public/attachments/FCC-26-29A1.pdf; *Id*. CISA ICSA-24-338-01.
[93] *Id*. paras. 13-16 (tentatively concluding that national security concerns support limits on interconnection with Covered List entities and seeking comment on prohibitions involving facilities including Points of Presence and data centers, existing agreements, transition periods, and possible retroactive application), https://docs.fcc.gov/public/attachments/FCC-26-29A1.pdf.
[94] Transcribed Interview of Witness # 6, at pp. 16-18 (Sept. 11, 2025).
[95] *Id.* at p. 17.
[96] S. Permanent Subcomm. on Investigations, 116th Cong., Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers (Comm. Print 2020), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.
[97] China Telecom (Americas) Corporation, Further Responses to Subpoena from the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party 8 (May 28, 2025) (identifying U.S. transmission-capacity agreements with CTA-SCCCP-000139 to CTA-SCCCP-000145; CTA-SCCCP-000146 to CTA-SCCCP-000227; CTA-SCCCP-000228 to CTA-SCCCP-000305; CTA-SCCCP-000306 to CTA-SCCCP-000310; CTA-SCCCP-000311 to CTA-SCCCP-000322; CTA-SCCCP-000323 to CTA-SCCCP-000395).
[98] Further Responses to Subpoena from the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party 8 (May 28, 2025); CTA-SCCCP-000396-000429 and CTA-SCCCP-000430-000453.
[99] Letter from China Telecom (Ams.) Corp. to Hon. John Moolenaar, Chairman, & Hon. Raja Krishnamoorthi, Ranking Member, H. Select Comm. on the Strategic Competition Between the U.S. & the Chinese Communist Party (May 28, 2025).
[100] Transcribed Interview of Witness # 4, at p. 29 (Sept. 29, 2025).
[101] Transcribed Interview of Witness # 2, at p. 21 (Sept. 17, 2025).
[102] Transcribed Interview of Witness # 2., at p. 17 (Sept. 17, 2025).
[103] CUA_HRCOMMCCP_0000584.
[104] U.S.-China Bus. Council, Ministry of Industry and Information Technology Organization Chart (Dec. 2020) (summarizing MIIT's telecommunications, software, electronics, information-technology manufacturing, and defense-industry related organizational responsibilities based on MIIT source material); State Council Info. Office of the People's Republic of China, China's Export Controls (Dec. 29, 2021) (describing China's export-control governance structure, including roles of the Ministry of Industry and Information Technology, the State Administration of Science, Technology and Industry for National Defense, and the Equipment Development Department of the Central Military Commission), https://english.www.gov.cn/archive/whitepaper/202112/29/content_WS61cc01b8c6d09c94e48a2df0.html.
[105] U.S.-China Economic and Security Review Commission, China's Global Police State: Background and U.S. Policy Implications, December 13, 2023, https://www.uscc.gov/sites/default/files/2023-12/Chinas_Global_Police_State.pdf.
[106] CUA_HRCOMMCCP_0000584.
[107] *Id*.
[108] Staff of Permanent Subcomm. on Investigations, S. Comm. on Homeland Sec. & Governmental Affairs, 116th Cong., Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers 29–31 (2020). *See* Yuval Shavitt & Chris C. Demchak, China's Maxim—Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking, Mil. Cyber Aff. art. 7 (2018).
[109] *Id*. at 31 (describing interception, the breaking of encryption on diverted traffic, and the difficulty of detection given unchanged latency).

[110] *Id.* at 31–32 (positioning in trusted networks).
[111] *Id*. at 3–5, 29–31, 65–69; Rahul Hiran, Niklas Carlsson & Phillipa Gill, Characterizing Large-Scale Routing Anomalies: A Case Study of the China Telecom Incident, in Passive and Active Measurement: 14th International Conference, PAM 2013, at 229, 229–38 (Matthew Roughan & Rocky K.C. Chang eds., 2013); Org. for Econ. Coop. & Dev., Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions 18–19 (2022).
[112] The announcement originated with AS23724, a China Telecom data center, which advertised approximately 37,000 prefixes, roughly 11 percent of all prefixes then in the global routing table. *See* U.S.-China Econ. & Sec. Review Comm'n, 2010 Report to Congress of the U.S.-China Economic and Security Review Commission, 111th Cong. 243–44 (2010), https://www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf.
[113] China Telecom (Americas) Corp., GN Docket No. 20-109, Order on Revocation and Termination, 36 FCC Rcd, at 15967, 15992 (2021), https://docs.fcc.gov/public/attachments/FCC-21-114A1_Rcd.pdf.
[114] Reporting on Border Gateway Protocol Risk Mitigation Progress, Notice of Proposed Rulemaking, FCC 24-62, WC Docket No. 24-146, at 1 (2024), https://docs.fcc.gov/public/attachments/FCC-24-62A2.pdf.
[115] China Unicom (Americas) Operations Ltd., GN Docket No. 20-110, Order on Revocation, 37 FCC Rcd 1480, ¶¶ 97–98 (2022), https://docs.fcc.gov/public/attachments/FCC-22-9A1_Rcd.pdf.
[116] China Unicom (Americas) Operations Ltd., GN Docket No. 20-110, Order on Revocation, 37 FCC Rcd 1480, ¶ 97 (2022), https://docs.fcc.gov/public/attachments/FCC-22-9A1_Rcd.pdf.
[117] China Mobile Int'l (USA) Inc., Memorandum Opinion and Order, 34 FCC Rcd 3361, at 3376–77 (2019), https://docs.fcc.gov/public/attachments/FCC-19-38A1_Rcd.pdf.
[118] Cybersecurity & Infrastructure Sec. Agency, Nat'l Sec. Agency, Fed. Bureau of Investigation et al., Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System, No. AA25-239A (Aug. 27, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.
[119] The Select Committee analyzed route announcements and withdrawals captured by the RIPE Network Coordination Centre's Routing Information Service, the Route Views Project, and Cloudflare Radar. It compared those announcements against public routing records for U.S.-associated IP address blocks and identified cases in which PRC or Hong Kong-associated carrier autonomous systems announced reachability for prefixes normally originated by U.S. networks. Counted events met four criteria: the announcing ASN was associated with a PRC or Hong Kong carrier; the affected prefix was associated with a U.S. network; the announcement either replaced the normal origin route or announced a more-specific prefix; and the event lasted at least one hour and was corroborated by an independent detection source. The Select Committee excluded events where public routing records showed a plausible authorization relationship. For each event, the Committee also reviewed Resource Public Key Infrastructure (RPKI) status to determine whether the announcing ASN had a matching Route Origin Authorization (ROA) for the affected prefix. Each counted event reflects a discrete route-origin observation, not a unique victim, prefix, or campaign. The underlying row-level dataset, offender-ASN watchlist, and filter parameters are preserved in the methodology annex. This baseline total was independently confirmed and verified by Cloudflare and outside cybersecurity experts. *See* RIPE NCC, Routing Information Service (RIS), https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris; University of Oregon Route Views Project, https://www.routeviews.org; Cloudflare, Cloudflare Radar, https://radar.cloudflare.com; Rahul Hiran, Niklas Carlsson & Phillipa Gill, Characterizing Large-Scale Routing Anomalies: A Case Study of the China Telecom Incident, in Passive and Active Measurement: 14th International Conference, PAM 2013, at 229 (Matthew Roughan & Rocky Chang eds., 2013); MANRS, Internet Soc'y, https://www.manrs.org; Kotikalapudi Sriram & Douglas Montgomery, Border Gateway Protocol Security and Resilience, NIST Special Pub. No. 800-189r1 (Initial Pub. Draft Jan. 3, 2025), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189r1.ipd.pdf.
[120] Staff Analysis of BGP Routing Data, Verified Hijack Incidents (Jan. 2018-June 2025) (on file with Select Committee).
[121] Select Committee analysis of historical Border Gateway Protocol routing data obtained from the University of Oregon Route Views Project and the RIPE Network Coordination Centre Routing Information Service, cross-referenced against network ownership and autonomous-system relationship data maintained by the Center for Applied Internet Data Analysis. See Route Views Project, RouteViews API Documentation, Univ. of Or., https://api.routeviews.org/docs/; Routing

Information Service, Route Collection Raw Data: MRT Files, RIPE Network Coordination Ctr., https://ris.ripe.net/docs/mrt/; Ctr. for Applied Internet Data Analysis, AS Rank: AS7018, https://asrank.caida.org/asns/7018; Ctr. for Applied Internet Data Analysis, AS Rank: AS9808, China Mobile, https://asrank.caida.org/asns/9808.

[122] Ctr. for Applied Internet Data Analysis, AS Rank: AS2914, https://asrank.caida.org/asns?asn=2914.

[123] Select Committee staff analysis of BGP routing data, June 2025 (on file with the Select Committee); Transcribed Interview of Witness # 4, p. 19. (Sept. 29, 2025); *id*. at pp. 24-25.

[124] Transcribed Interview of Witness #5, at p. 91 (Sept. 10, 2025); Transcribed Interview of Witness #4, at p. 31 (Sept. 29, 2025); Transcribed Interview of Witness #2, at p. 27 (Sept. 17, 2025).

[125] Nat'l Inst. of Standards & Tech., *Border Gateway Protocol Security and Resilience*, NIST SP 800-189 Rev. 1, Initial Public Draft (Jan. 2025); Org. for Econ. Coop. & Dev., Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions 18–19 (2022).

[126] The U.S. government placed Qihoo 360 on the Commerce Department's Entity List on June 5, 2020, and designated it a Chinese military company under Section 1260H of the FY2021 National Defense Authorization Act on October 5, 2022, *see* Commerce Department to Add Two Dozen Chinese Companies with Ties to WMD and Military Activities to the Entity List, U.S. Dep't of Com. (May 22, 2020); Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), U.S. Dep't of Def. (Jan. 7, 2025).

[127] Jiang Jie, China Unveils Its First Civil-Military Cybersecurity Innovation Center, People's Daily Online (Dec. 28, 2017), https://perma.cc/F4UX-H8YB.

[128] 360: Consciously Take Responsibility to Safeguard Cybersecurity [360：自觉担当责任维护网络安全], Cyberspace Admin. of China (Nov. 6, 2018), https://perma.cc/ENA2-WZ3F.

[129] China National Vulnerability Database of Information Security [国家信息安全漏洞库], https://perma.cc/F6PM-MT8H; Priscilla Moriuchi & Bill Ladd, China Altered Public Vulnerability Data to Conceal MSS Influence, Recorded Future (Mar. 9, 2018), https://www.recordedfuture.com/blog/chinese-vulnerability-data-altered.

[130] Winnona Bernsen, Same Same, but Different, Margin Rsch. (Feb. 29, 2024), https://perma.cc/523F-74F2; WithSecure, Threat Landscape Update. February 2024, at 16 (Mar. 4, 2024) (summarizing Margin Research's conclusion that Qihoo 360 may be selling personal information of individual antivirus customers to a Qihoo-funded company working for Chinese government intelligence clients); SentinelOne, Unmasking I-Soon. The Leak That Revealed China's Cyber Operations (Feb. 21, 2024) (describing the i-SOON leak as revealing a Chinese government-driven hacker-for-hire ecosystem); Tom Uren & Catalin Cimpanu, The I-Soon Data Leak + Disruption, Disruption Everywhere, Lawfare (Feb. 23, 2024), https://www.lawfaremedia.org/article/the-i-soon-data-leak-disruption-disruption-everywhere (describing leaked files suggesting i-Soon carried out cyber espionage on behalf of the Chinese government).

[131] Margin Rsch., The Chinese Private Sector Cyber Landscape (Apr. 25, 2022) (reporting a possible Qihoo 360 link to a U.S. insurance company hack). The Select Committee treats this as a reported private-sector analytic claim. Public U.S. government materials concerning the breach attribute the operation to Chinese state-affiliated actors but do not identify Qihoo 360 as the responsible entity.

[132] BGP Adjacency Analysis: Qihoo 360 (AS55992) peering with China Telecom Americas (AS36678), RIPE NCC RIS Data, 716 direct adjacency observations, Sept. 22-23, 2024 (on file with Select Committee).

[133] ARIN WHOIS Registration Records for 104.192.108.0/22, QiHu 360 Inc. (on file with Select Committee).

[134] Sarah Krouse, Robert McMillan & Dustin Volz, *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, Wall Street Journal (Sept. 26, 2024), https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

[135] Based on Select Committee observations, the two networks had a Pearson correlation of 0.53 and a Spearman rank correlation of 0.35, with both results significant at $p < 0.001$.

[136] Shodan and Censys scan data for AS55992 prefixes, including Shodan query results for ports 8282, 8888, 8989, 9899, and UDP 500; WoTrus Certificate Transparency logs; Analysis of Censys and Shodan Network Scan Data (all on file with Select Committee).

[137] Shodan Historical Scan Comparison: Qihoo 360 U.S. IP Blocks, Aug.-Sept. 2024 (on file with Select Committee).

[138] Cybersecurity Advisory, CISA, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*, September 03, 2025,

https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

[139] Press Release, Fed. Bureau of Investigation, *Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure* (Nov. 13, 2024), https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure.

[140] Christopher A. Wray, Director, Fed. Bureau of Investigation, Remarks for the FBI All-Employee Town Hall Address (Dec. 11, 2024), https://www.fbi.gov/news/speeches-and-testimony/director-wrays-remarks-for-the-fbi-all-employee-town-hall-address (describing Salt Typhoon as potentially "the PRC's broadest, most significant cyber espionage campaign in history").

[141] Lee Neubecker, *China-Affiliated ISPs in the U.S. Create Beachhead for North Korean Cyber Attacks Against U.S. Assets*, EIN Presswire (May 23, 2017), https://www.einpresswire.com/article/382795538; CloudRadium (HK) Limited, AS17476 WHOIS Record, APNIC (last modified Mar. 15, 2024) (as-name CHL-AS-AP; org CloudRadium (HK) Limited; country HK); CloudRadium (HK) Limited, PeeringDB (last updated Apr. 25, 2025).

[142] GlobalData Investments Inc., Articles of Incorporation, Entity No. 4145728 (Cal. Sec'y of State filed May 4, 2018); GlobalData Investments Inc., Statement of Information, File No. BA20260846933 (Cal. Sec'y of State filed Apr. 17, 2026); CloudRadium L.L.C., Business Entity Detail, Filing ID 2012-000630312, Wyo. Sec'y of State; CeraNetworks, Contact Us, https://perma.cc/S4VS-2G2M. Of note, GlobalData acquired CeraNetworks LLC, folding its assets into a footprint it markets as seven datacenters and nine points of presence across North America and the Asia Pacific, *see* GlobalData Investments Inc. Acquires CeRaNetworks LLC, CeraNetworks, https://perma.cc/5XSF-G6HC.

[143] CloudRadium L.L.C., Business Entity Detail, Filing ID 2012-000630312, Wyo. Sec'y of State (initial filing Oct. 1, 2012); Transcribed Interview of Witness # 1, at p.13 ln. 21 (Sept. 17, 2025).

[144] *See*, e.g., China Mobile Int'l Ltd., Order Form – IP Transit/DIA Service (CloudRadium L.L.C.), CMI-B-2024-46066 (executed Feb. 5, 2024) (Bates CMIUSA_HC_0000545–550); *id*., CMI-B-2024-47513 (executed Mar. 27, 2024) (Bates CMIUSA_HC_0000563–568); *id*., CMI-B-2024-48229 (executed Apr. 22, 2024) (Bates CMIUSA_HC_0000575–580); *id*., CMI-B-2024-52619 (executed Aug. 26, 2024) (Bates CMIUSA_HC_0000581–586, _0000593–598); *id*., CMI-B-2024-52899 (executed Sept. 5, 2024) (Bates CMIUSA_HC_0000611–616); *id*., CMI-B-2025-62040 (executed May 27, 2025) (Bates CMIUSA_HC_0000617–622) (all produced to the Select Comm. pursuant to subpoena).

[145] *See, e.g.*, CMI-B-2024-46066, § 3, at 2 (Bates CMIUSA_HC_0000546) ("BUYER acknowledges and agrees the Service is provided by a service provider. SELLER is an AGENT of BUYER located outside Service Location . . . and SELLER does not execute this Order Form in Service Location.").

[146] *Compare id*., CMI-B-2024-46066, at 2 (Bates CMIUSA_HC_0000546), with *id*., CMI-B-2025-62040, at 2 (Bates CMIUSA_HC_0000618).

[147] *Compare id.*, CMI-B-2024-46066, at 2 (Bates CMIUSA_HC_0000546), with *id*., CMI-B-2025-62040, at 2 (Bates CMIUSA_HC_0000618).

[148] *Id*., CMI-B-2025-62040, § 4, at 4 (Bates CMIUSA_HC_0000620) (48-month term; MRC $10,000; TCV $480,000; "该线路与所有美国 CM-ON-NET IP 线路合并计费" [this line is billed jointly with all U.S. CM-ON-NET IP lines]).

[149] *Id*., CMI-B-2024-46066X, at 2 (Bates CMIUSA_HC_0000600) ("本条线路是 US 扩容 10 条中的 1 条, 由于 LA 没有资源, 暂时在 SanJose 开通, LA 有资源后迁回 LA" [this line is 1 of 10 in the U.S. expansion; because LA lacks resources, temporarily activated in San Jose, to migrate back to LA when resources are available]).

[150] *Compare id*., CMI-B-2025-62040, at 6 (Bates CMIUSA_HC_0000622) (countersigned by Colin Wang Yizhou, Division Head, China Mobile Int'l Ltd., May 27, 2025).

[151] CMI is formally registered as an "upstream" provider for AS17476 (CloudRadium), while CMI's own internal documentation mirrors this by designating AS17476 as a "downstream" client, confirming a reciprocal routing relationship. This partnership is further corroborated by additional subpoenaed circuits operating under AS40065, a secondary autonomous system associated with CloudRadium, demonstrating that the connectivity was not confined to a single routing path, *see* AS17476 CloudRadium (HK) Limited, bgp.tools, https://bgp.tools/as/17476 (last updated Dec. 31, 2024) (listing AS58453 China Mobile International among upstreams); AS58453 China Mobile International, Ipregistry, https://ipregistry.co/AS58453 (listing AS17476 among downstreams); CMIUSA_HC_0000547.

[152] Lee Neubecker, Wanna Crypt Malware Begins US Assault, LEE NEUBECKER (May 15, 2017), https://glforensics.wpengine.com/wanna-crypt-malware-assaults-us/ (reporting 42,973 results geolocated to Cheyenne, Wyoming); Lee Neubecker, 70%+ of US Wanna Cry Malware Exposure

Linked to 35 ISPs, LEE NEUBECKER (May 17, 2017), https://leeneubecker.com/majority-exposure-wanna-cry-35-isps/ (reporting 42,746 CloudRadium results among 499,402 United States results, or 8.56 percent).

[153] Lee Neubecker, China Infiltration of U.S. ISPs Creates Beachhead for Cyber Attacks, LEE NEUBECKER (May 23, 2017), https://leeneubecker.com/china-us-isp-invasion/ (reporting that most Cheyenne results used IP addresses associated with CloudRadium); Search Query Fundamentals, SHODAN HELP CTR., https://help.shodan.io/the-basics/search-query-fundamentals (explaining that Shodan collects service banners containing IP address, organization, and location information).

[154] Press Release, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, US Dept. of Justice, September 6, 2018, https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[155] *Id*.; Jon Condra, John Costello & Sherman Chu, Linguistic Analysis of WannaCry Ransomware Messages Suggests Chinese-Speaking Authors, Flashpoint (May 25, 2017), quoted in Kelly Jackson Higgins, WannaCry Ransom Notes Penned by Chinese Speaking Authors, Analysis Shows, Dark Reading (May 25, 2017), https://www.darkreading.com/threat-intelligence/wannacry-ransom-notes-penned-by-chinese-speaking-authors-analysis-shows.

[156] Press Release, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), U.S. Dep't of Just., https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (reporting that the FBI traced North Korean, Chinese, and other IP addresses and found that some malicious infrastructure was used across multiple operations); Criminal Complaint ¶¶ 284, 310, 333(g), United States v. Park Jin Hyok, No. 18-MJ-1479 (C.D. Cal. June 8, 2018), https://www.justice.gov/archives/opa/press-release/file/1092091/dl (identifying IP addresses registered to China Unicom Liaoning that were used by accounts connected to Park and Chosun Expo).

[157] Identifying WannaMine command-and-control servers at 172.247.116.8 and 172.247.166.87 hosted by CloudRadium L.L.C., *see* Collin Montenegro & Mark Robinson, Weeding out WannaMine v4.0: Analyzing and Remediating This Mineware Nightmare, CrowdStrike (Nov. 12, 2019), https://www.crowdstrike.com/en-us/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/; Sean Gallagher, *Unpatched Systems at Big Companies Continue to Fall to WannaMine Worm*, Ars Technica (Sept. 14, 2018), https://arstechnica.com/information-technology/2018/09/eternally-pwned-wannamine-still-spreading-using-year-old-leaked-nsa-exploits/.

[158] Sean Gallagher, *Unpatched Systems at Big Companies Continue to Fall to WannaMine Worm*, Ars Technica (Sept. 14, 2018), https://arstechnica.com/information-technology/2018/09/eternally-pwned-wannamine-still-spreading-using-year-old-leaked-nsa-exploits/.

[159] Lists CloudRadium among the top ten hosters of fake shops in 2021, with 2,342 attack campaigns and a 2.18 percent share, *See* Nat'l Cyber Sec. Ctr. (U.K.), *Active Cyber Defence: The Fifth Year*, tbl. 10 (May 2022), https://www.ncsc.gov.uk/files/ACD-the-fifth-year.pdf.

[160]About Us [关于我们], Integrity Technology Group [永信至诚], archived at Internet Archive Wayback Machine (May 23, 2024), https://web.archive.org/web/20240523041310/https://integritytech.com.cn/html/about/about-us/. For background on cyber ranges, see The Cyber Range: A Guide, National Institute of Standards and Technology (Sept. 2023), https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf; Dakota Cary, Downrange: A Survey of China's Cyber Ranges, Center for Security and Emerging Technology (Sept. 2022), https://cset.georgetown.edu/wp-content/uploads/CSET-Downrange-A-Survey-of-Chinas-Cyber-Ranges-1.pdf.

[161]Integrity Technology Group Lists on the STAR Market [永信至诚登陆科创板], Securities Times [证券时报网] (Oct. 19, 2022), https://perma.cc/EG6H-KKY2. The firm's 2025 semiannual report reframes the same intelligence collection and reconnaissance services as provided to "relevant government departments" at the national and provincial-municipal levels, a softer formulation postdating the sanctions. See Integrity Technology Group Inc., 2025 Semiannual Report [2025年半年度报告], CNINFO [巨潮资讯网] (Aug. 29, 2025), https://static.cninfo.com.cn/finalpage/2025-08-29/1224606774.PDF.

[162]Integrity Technology Group Inc. [永信至诚科技集团股份有限公司], 2023 Annual Report [2023年年度报告] (Apr. 29, 2024), https://static.sse.com.cn/disclosure/listedinfo/announcement/c/new/2024-04-29/688244_20240429_3RO3.pdf; Press Statement, Matthew Miller, Spokesperson, U.S. Dep't of State,

Sanctioning PRC Cyber Company Involved in Malicious Botnet Operations (Jan. 3, 2025), https://2021-2025.state.gov/sanctioning-prc-cyber-company-involved-in-malicious-botnet-operations/.
[163]State-Owned Capital-Backed Professional Fund Leads Investment as Integrity Technology Group Completes RMB 200 Million Financing [国资背景专业基金领投，永信至诚完成2亿元融资], Integrity Technology Group [永信至诚] (Dec. 4, 2020), archived at Internet Archive Wayback Machine, https://web.archive.org/web/20201204020305/http://www.integritytech.com.cn/html/News/News_489_1.html.
[164]Fed. Bureau of Investigation, Cyber Nat'l Mission Force & Nat'l Sec. Agency et al., People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations 1 (Sept. 18, 2024), https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF.
[165]*Id*. at 3.
[166]*Id*. at 3–4.
[167]*Id*. at 3.
[168]Application for Search Warrant, In re: Search of Information Associated with the "Integrity Technology Group" Botnet Infrastructure, No. 24-mj-1484 (D.D.C. Sept. 2024), https://www.justice.gov/d9/2024-09/redacted_24-mj-1484_signed_search_and_seizure_warrant_for_disclosure.pdf.
[169]Press Release, Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers, U.S. Dep't of Justice (Sept. 18, 2024), https://www.justice.gov/usao-wdpa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state; Press Release, Treasury Sanctions Technology Company for Support to Malicious Cyber Group, U.S. Dep't of the Treasury (Jan. 3, 2025), https://home.treasury.gov/news/press-releases/jy2769.
[170]Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation, Recorded Future, Insikt Group (June 24, 2024), https://www.recordedfuture.com/research/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter; Ethereal Panda, CrowdStrike, https://www.crowdstrike.com/en-us/adversaries/ethereal-panda/; Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations, Microsoft Threat Intelligence (Aug. 24, 2023), https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/.
[171]*Id*. (Recorded Future), Insikt observed suspected administration activity from Chinanet IP addresses geolocating to Fuzhou, Fujian province, and assessed that the group likely operates from that city.
[172]The overlap between the Fuzhou geolocation and Integrity Tech's office in the Fuzhou Software Park was first drawn by the Natto Team. See Flax Typhoon-Linked Company Integrity Technology: A Competitor, Business Partner and Client of i-SOON, Natto Thoughts (Sept. 25, 2024), https://nattothoughts.substack.com/p/flax-typhoon-linked-company-integrity.
[173]White Paper on the Practical Capabilities of Cybersecurity Talent—Security Testing and Assessment Volume Officially Released [《网络安全人才实战能力白皮书——安全测试评估篇》正式发布], Integrity Technology Group Inc. (Sept. 10, 2024), https://www.integritytech.com.cn/html/News/News_743_1.html.
[174]Adam Kozy, Testimony Before the U.S.-China Economic and Security Review Commission 4–5 (Feb. 17, 2022), https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf.
[175]Investor Relations Activity Record No. 2024-001 [投资者关系活动记录表（编号：2024-001）], Integrity Technology Group Inc. (Jan. 12, 2024), https://pdf.dfcfw.com/pdf/H22_AN202401121617323164_1.pdf.
[176]December 2023 China Unicom Software Research Institute Information Security Operations Domain Practical Attack-and-Defense Exercise System Procurement Results [2023年12月中国联通软研院信息安全运营域实战攻防演练系统采购结果], International Tendering Network [必联网] (Dec. 21, 2023), https://perma.cc/DEE3-XJ6G; 2025 China Unicom Software Research Institute Application Security Practical Attack-and-Defense Exercise System Procurement Project Evaluation Results Notice [2025年中国联通软研院应用安全实战攻防演练系统购置项目评审结果公示], China CNTC International Tendering Co. (July 23, 2025), https://perma.cc/3YSW-UN98.
[177]China Unicom 2025–2027 Network Security and Data Security Competition Services Selected-Candidate Notice [2025-2027年中国联通网络安全及数据安全竞赛服务中选候选人公示], China CNTC International Tendering Co. (June 24, 2025), https://perma.cc/4NAA-4RYQ.

[178]Corporate Cooperation Partners [合作伙伴：企业合作], i-SOON [安洵信息], archived at Internet Archive Wayback Machine (Feb. 19, 2024), https://web.archive.org/web/20240219105958/http://www.i-soon.net/firm_partner.html; Indictment ¶ 6, United States v. Wu Haibo, No. 24 Cr. 687 (S.D.N.Y. unsealed Mar. 5, 2025), https://www.justice.gov/usao-sdny/media/1391751/dl?inline=.

[179]Indictment, United States v. Wu Haibo, No. 24 Cr. 687 (S.D.N.Y. unsealed Mar. 5, 2025); see also Press Release, 10 Chinese Nationals Charged With Large-Scale Hacking of U.S. and International Victims on Behalf of the Chinese Government, U.S. Dep't of Justice, S.D.N.Y. (Mar. 5, 2025), https://www.justice.gov/usao-sdny/pr/10-chinese-nationals-charged-large-scale-hacking-us-and-international-victims-behalf.

[180]Press Release, Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign, U.S. Dep't of Justice (July 19, 2021), https://www.justice.gov/archives/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion (attributing APT40 to the Hainan State Security Department); Press Release, Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, U.S. Dep't of Justice (Dec. 20, 2018), https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion (attributing APT10 to the Tianjin State Security Bureau).

[181]China Unicom Digital Technology's Cybersecurity Large Language Model Selected for Beijing's Major First-of-a-Kind Technical Equipment Catalog [联通数科网络安全大模型入选北京首台（套）重大技术装备目录], People's Daily Online [人民网] (Sept. 16, 2025), http://finance.people.com.cn/n1/2025/0916/c1004-40565286.html.

[182] *China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd. 3361 (2019); *China Telecom (Americas) Corp.*, Order on Revocation and Termination, 36 FCC Rcd. 15966 (2021); *China Unicom (Americas) Operations Ltd.*, Order on Revocation, 37 FCC Rcd. 1480 (2022). See also 47 U.S.C. § 214.

[183] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (codified as amended at 47 U.S.C. §§ 1601–1609); Exec. Order No. 13,913, 85 Fed. Reg. 19,643 (Apr. 8, 2020); Securing the Information and Communications Technology and Services Supply Chain, 15 C.F.R. pt. 791; Cybersecurity & Infrastructure Security Agency, *Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide*, Alert AA25-239A (Aug. 27, 2025).

[184] Protecting Against National Security Threats in Domestic Telecommunications Service, Notice of Proposed Rulemaking, WC Docket No. 26-82, FCC 26-29, paras. 7-8, 11-18, 19-22 (rel. May 1, 2026), published at 91 Fed. Reg. 25325, (May 8, 2026), paras. 13-16 (tentatively concluding that national security concerns support limits on interconnection with Covered List entities and seeking comment on prohibitions involving facilities including Points of Presence and data centers, existing agreements, transition periods, and possible retroactive application), https://docs.fcc.gov/public/attachments/FCC-26-29A1.pdf.