ABUSING DATA IN THE MIDDLE

Surveillance Risks in China's State-Owned Mobile Ecosystem

iVerify.

iverify.io

TABLE OF CONTENTS

Executive Summary

This report explores the cybersecurity risks posed by China's state-owned mobile interconnect providers, such as China Mobile International (CMI) and China Telecom Global. Although these providers play an important role in the global mobile ecosystem, they also introduce significant risks due to their transport of unencrypted signaling protocols like SS7 and Diameter, coupled with concerns stemming from state ownership and control.

A major issue lies in the fact that these providers operate under the direction of the Chinese government, raising the risk of global surveillance, data interception, and exploitation for state-sponsored cyber espionage. Their role in the mobile interconnect system grants them access to critical functions, including device authentication, call setup, SMS delivery, location updates, and data session management—making them prime channels for exploiting network vulnerabilities.

The technical risks originate from the outdated nature of telecom signaling protocols, initially designed decades ago without encryption lacking an industry focus on security. These protocols handle essential mobile network functions, but their lack of security leaves them vulnerable to multi-vector attacks, enabling malicious actors to intercept, manipulate, or inject spoofed traffic into mobile networks.

Multiple threat actors, including foreign agencies, APT groups, and cybercriminals, have previously exploited these vulnerabilities. In a high-profile investigation by The Guardian in December 2020, a surveillance operation by Chinese actors targeting US mobile users through foreign networks that leveraged US carrier roaming agreements was exposed. These attacks, originating from foreign SS7 addresses, led to multiple US agency disclosures and congressional inquiries. Some of the attacks were traced to Huawei equipment at foreign operator networks. An earlier incident in 2017 exploited SS7 to intercept SMS two-factor authentication (2FA) codes, leading to the theft of funds from multiple bank accounts in Germany.

Threat actors routinely abuse mobile network vulnerabilities to track the real-time location of devices, push over-the-air (OTA) updates to covertly install spyware, or take over WhatsApp accounts. They can also carry out highly targeted SMS phishing (smishing) attacks.

For cybersecurity professionals, defending against these threats presents significant OPSEC challenges, as mobile operators must open a range of signaling interfaces and protocols to foreign networks, including those who provide access to 3rd parties, bypassing traditional security measures.. China's state-controlled interconnect providers,

Introduction

A 2024 Deloitte survey found that nearly half of Americans planned to travel for the holidays, with a growing share of those trips being international. However, as international travel rises, so does the risk of exposure to the secret tradecraft of mobile surveillance tactics enabled by foreign interconnect providers.

The infiltration of global telecom networks by Chinese actors highlights a long-standing but underreported reality long-known by mobile telecom insiders—security threats extend far beyond legacy SS7 vulnerabilities. Though SS7 threats are pervasive in developing countries, the broader security risk lies in the intricate web of interconnections linking mobile operators worldwide. While essential for international roaming, it also serves as a gateway for surveillance actors to monitor signaling traffic, exploit multiprotocol vulnerabilities, and establish persistent access to virtually every mobile network on the planet. These are not theoretical risks, but active threats, allowing state-backed operators to track, intercept, and manipulate mobile communications with precision.

Background

The GSMA refers to China Mobile International as “a trusted partner that provides comprehensive international information services and solutions to international enterprises, carriers and mobile users.” However, CMI is owned by the PRC, and in 2022 under the Secure Networks Act, it was added to the FCC’s list of service providers and deemed as a threat to US national security.

The FCC decision followed US government investigations, one of which found that China Telecom had misrouted US internet traffic through China, putting it at risk of interception by Chinese authorities. In addition, a 2021 Crowdstrike report-updated in November revealed tooling used by the China-based LIMINAL PANDA threat group to exploit mobile roaming interconnects to access operator core networks.

Analysis of recent data from mobile operators around the world reveals China’s role as a globally significant mobile interconnect provider. This role provides them with access to highly sensitive mobile network and user traffic, extending beyond individual attacks to more systemic global security risks.

Key Findings

According to operational documents submitted by mobile network operators to the GSMA known as IR.21 RAEX (Roaming Agreement EXchange), 60 operators from 35 countries have been identified using the following China and Hong Kong-based networks for transporting mobile user traffic:

- China Mobile International (CMI)
- China Telecom Global
- China Unicom Global (CUG)
- CITIC Telecom International
- PCCW Global Hong Kong

Of the mobile operators using China networks, many are located in countries of US allies including Japan, Saudi Arabia, South Korea, Taiwan, and 2 mobile networks of Five Eyes intelligence partner New Zealand.

Interconnect services provided by China operators include the transport of highly sensitive signaling data used in device authentication, call setup, SMS, network location updates, setting up data sessions, and transporting internet data for international travelers.

Because mobile signaling protocols are not encrypted, the data is highly visible, providing China networks with “man in the middle” access to sensitive user device, service, and network information.

Overview of Mobile Interconnect Services

Today, more than 1000 mobile network operators (MNOs) operate 3G, 4G, and 5G networks across the globe. To enable seamless services beyond country borders, agreements and secure connectivity is required between hundreds of foreign mobile operators. To protect user traffic, the industry adopted a private network backbone designed to ensure security, scalability, and efficiency to minimize the operational and cost burdens of maintaining hundreds of direct connections. This gave rise to an ecosystem of SS7 and IPeXchange (IPX) interconnect providers.

Originally conceived as a trusted community of wholesale telecom providers, the IPX model centralizes the transport of multiprotocol signaling and services with a seamless mobile operator interconnect chain. However, the seamless chain has transformed into a “kill chain” exploited by persistent cyber threat groups carrying out targeted surveillance activity. Operating outside the reach of conventional managed security providers and threat intelligence tools, attackers take advantage of inherent vulnerabilities in the interconnect backbone. In the realm of telecom cyberattacks, China stands as the most advanced player, with over 15 APT groups linked to sophisticated campaigns aimed at digital espionage and mass harvesting of mobile user data globally.

How it Works

Mobile interconnect networks like the IPX were designed as private, service-aware hub-and-spoke network architectures, enabling mobile operators to form 3rd party agreements with network providers, to establish multilateral connections to other foreign mobile operators. By acting as a proxy, the IPX provider exchanges mobility signaling data and user service traffic, primarily to facilitate roaming.

To provide global reach, the IPX connects to other IPX networks through peering points as a service hub for routing device authentication, mobility management, and service traffic. A single operator may use multiple interconnect providers based on operational needs, creating a complex web of interconnections. The diagram below shows a basic representation of this model.

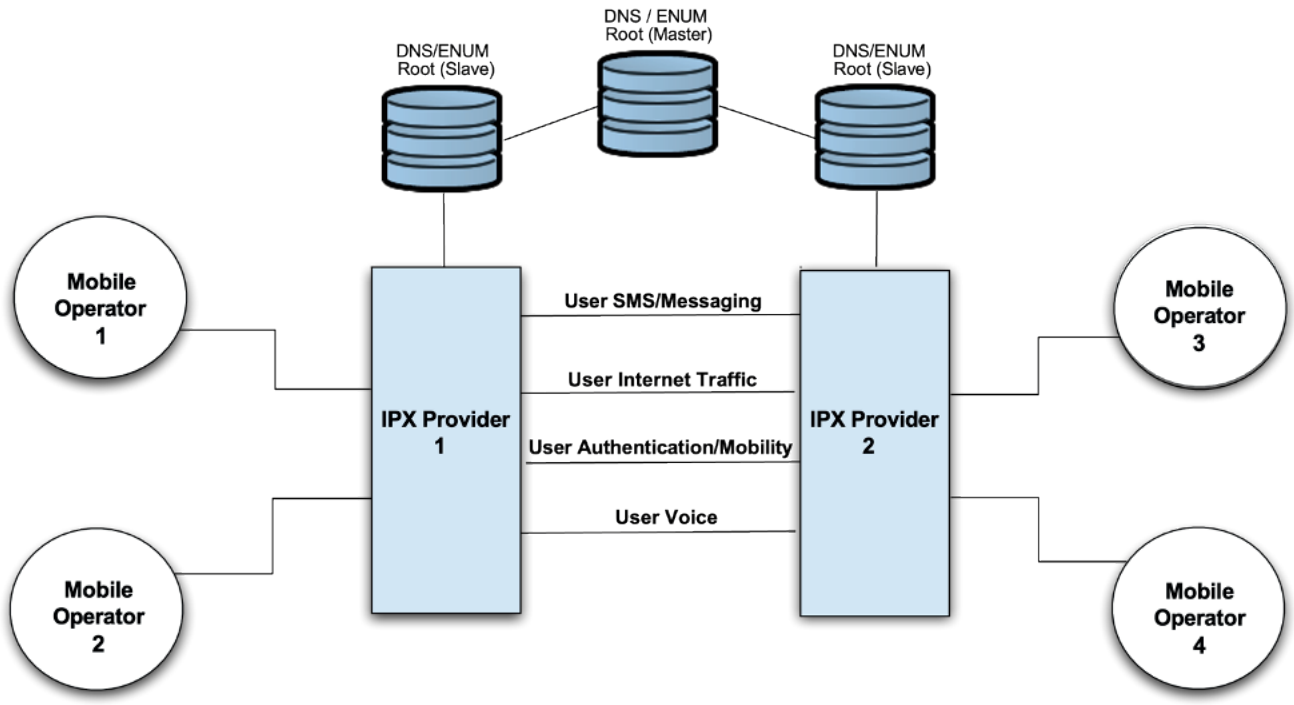

Figure 1. IPX Mobile Interconnect Service Model

The GSMA requires full data transparency within the IPX ecosystem, meaning user traffic may traverse through multiple interconnect providers based on traffic routing information. For instance, traffic from a subscriber of Mobile Network Operator 1 roaming on Mobile Network Operator 3's network passes through IPX 1 and 2, exposing various user data types to both IPX providers along the routing path.

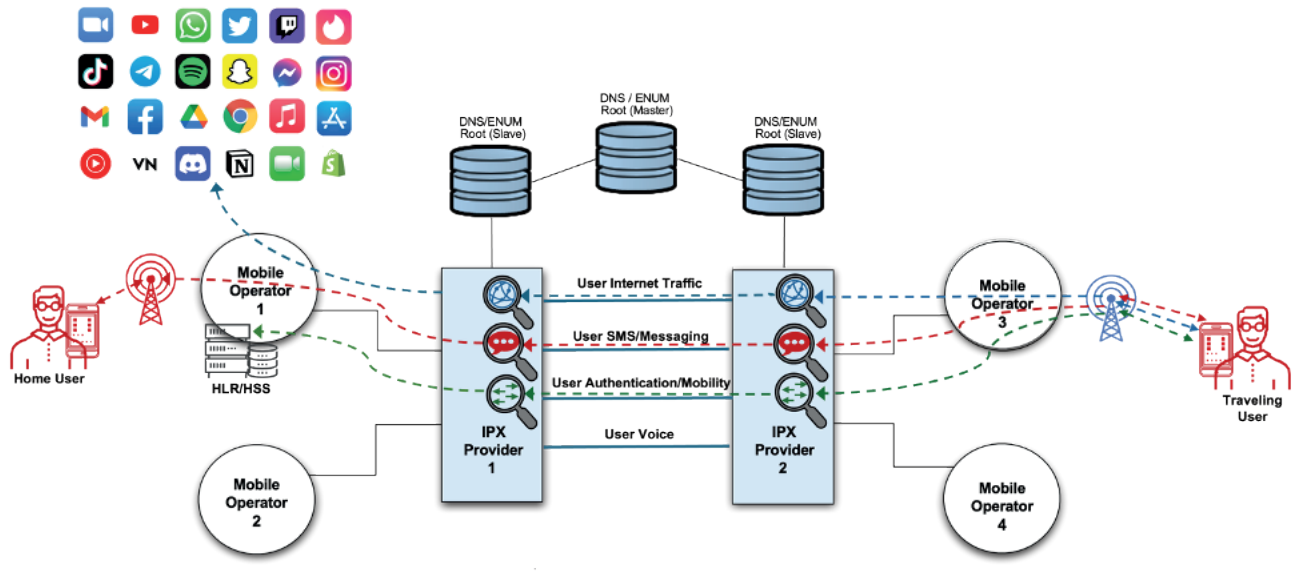

Figure 2. Traffic Exposure to IPX Providers During International Travel

Where's the Security?

Since its inception, the concept of user privacy for international mobility has been more of an afterthought. IPX security documents such as GSMA IR.77 have stated that traffic encryption measures are "not seen as necessary in an inter-operator network, as the network itself is secure and transparent." However, this assumption has proven to be dangerously flawed.

SS7 and IPX internetworks have repeatedly demonstrated vulnerabilities that undermine statements of security and transparency. Several factors play a role, but a significant issue lies in the widespread practice of mobile operators that lease network access and mobile signaling addresses to 3rd parties who present themselves as legitimate mobile service providers. These arrangements have created exploitable security gaps that far outweigh their operational benefits.

Adding to the risks, numerous international espionage firms, such as Fink Telecom, Tykelab, Picsix, Rayzone Group, and Septier Communications offer embedded telecom surveillance services. These firms, coupled with state-sponsored APT groups, leverage pools of leased SS7 and Diameter addresses to carry out attacks, raising the need for a critical assessment of mobile interconnect security.

Attack Vectors

Chinese IPX networks, with direct and indirect connections to mobile operators can provide a surveillance toolkit to the PRC for meeting surveillance objectives. Their central role within the mobile telecom ecosystem enables state-controlled networks to engage in passive and active surveillance operations, or even facilitate malware distribution through vulnerable network interfaces.

For Passive Surveillance Operations

As intermediaries connecting mobile networks, IPX providers can use passive techniques to intercept, capture, and store unencrypted traffic transiting the network using DPI tools and data collectors, providing mass surveillance with granular insights into individual user activity. Because IPX is designed for 3G, 4G, and 5G Non-standalone (NSA) network technologies, data captures can build a complete picture of users and the operator network components serving them.

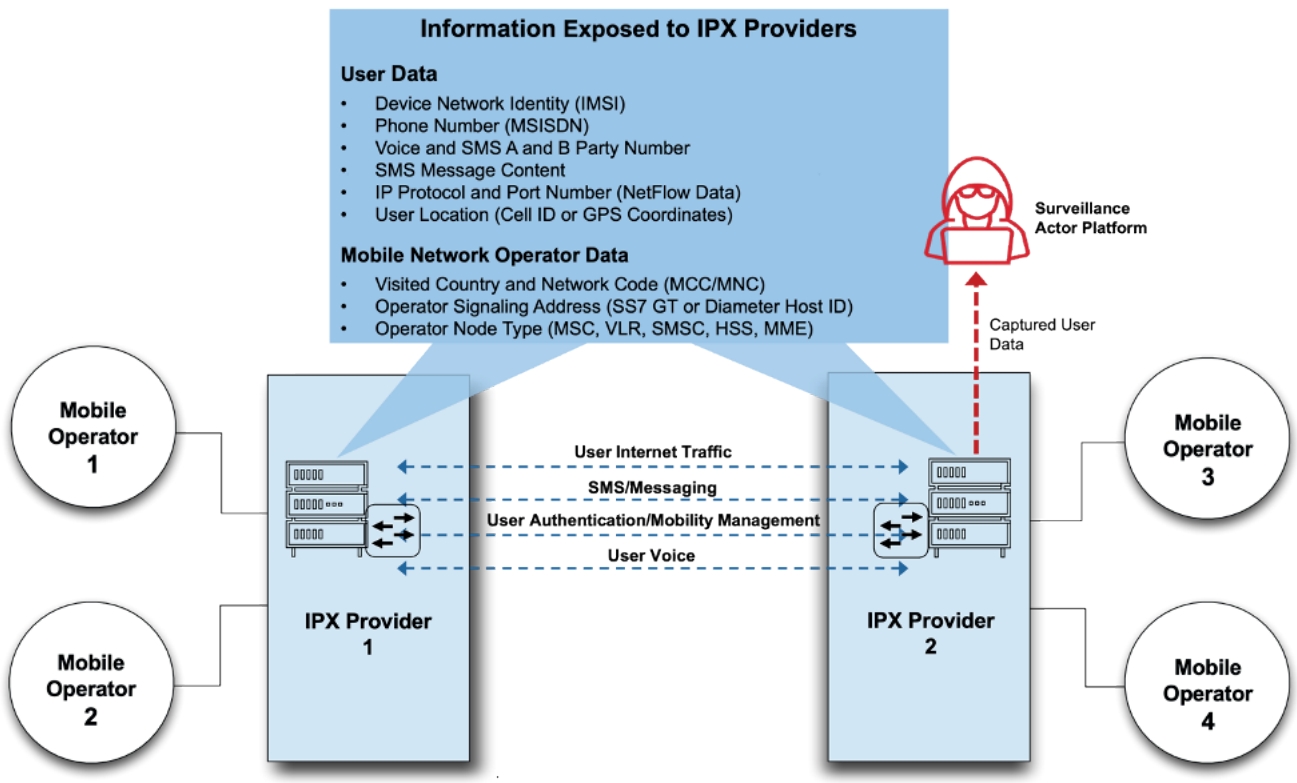

Figure 3. Key Information Exposed to Passive Interception Tools

Through data harvesting practices suspected by China state-sponsored threat groups, passive data captured by the IPX offers large-scale intelligence gathering. When combined with AI-driven inference techniques, the data can provide advanced user profiling capabilities including:

- Tracking travel durations and movement patterns.
- Monitoring user footfall data to create geofences around sensitive areas, user hotels, or corporate offices.
- Identifying business vs leisure travel.
- Detecting when a device is powered on or off at specific times or locations.
- Identifying inbound or outbound flight details.
- Determining whether a user is co-traveling with others.
- Detecting VPN or encrypted communications usage to evade monitoring.
- Building behavioral profiles and inferring socioeconomic status based on app and data usage patterns.

For Active Surveillance Operations

By exploiting private mobile network DNS resolution, operator network control interfaces, and traffic routing manipulation, adversaries can access a broad attack surface for targeted signaling attacks via IPX hosted connections. An attacker covertly injects signaling commands into the IPX backbone directed to the victim's home network using leased pools of 3G Global Titles and 4G Diameter host addresses from multiple foreign networks. By disguising the signaling message as a legitimate source, the attacker maintains anonymity. The IPX provider can then manipulate the reply path, routing responses to the surveillance platform instead of the mobile network assigned to the signaling address. Signaling commands offer real-time location tracking, denial-of-service, communication interception, and device data extraction, providing persistent surveillance capabilities to state-actors. In the example below, a combination of 3G and 4G signaling addresses and commands can be dynamically orchestrated into cross-protocol attack techniques designed to bypass operator firewalls.

Message 1 – Attempt Location Tracking using SS7 *anyTimeInterrogation (ATI)*

Message 2 – Attempt Location Tracking using Diameter *Insert-Subscriber-Data-Request (IDR)*

Message 3 – Attempt Denial of Service using SS7 *deleteSubscriberData (DSD)*

Message 4 – Attempt Denial of Service using Diameter *Cancel-Location-Request (CLR)*

Message 5 – Attempt Comms Interception using SS7 *updateLocation (LU)*

Message 6 – Attempt Comms Interception using Diameter *Update-Location-Request (ULR)*

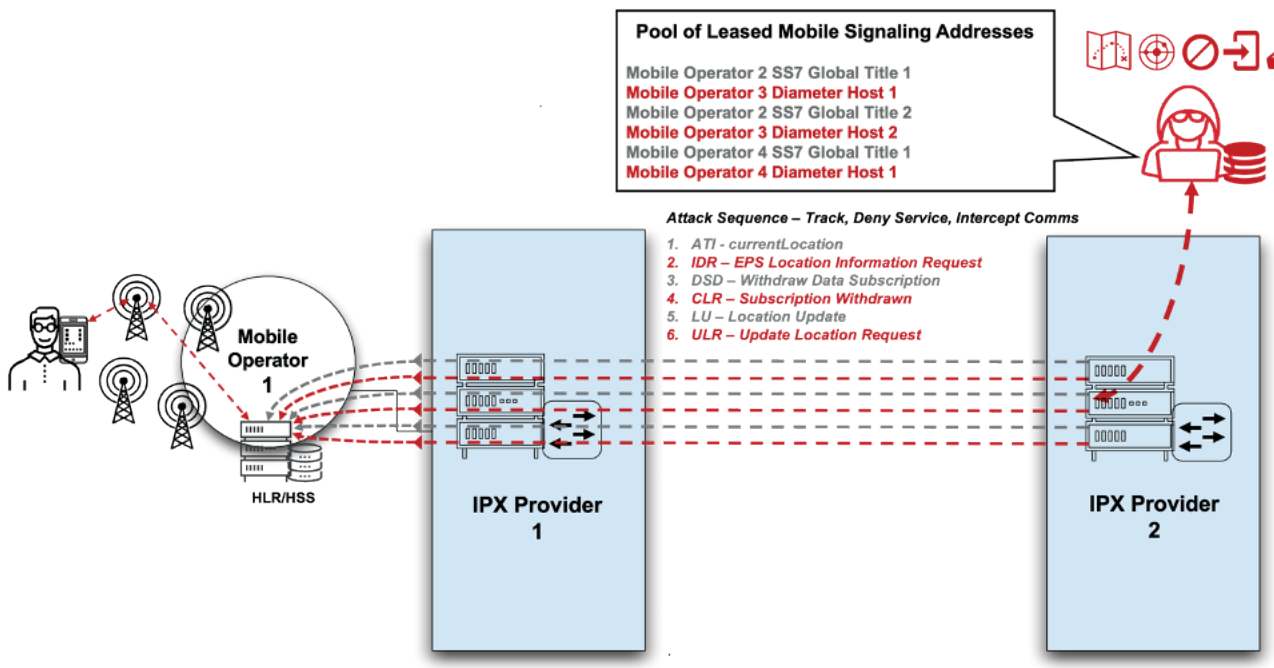

Figure 4. Active Signaling Surveillance Flow

For Malware Distribution

Host addresses of operator core network components and application types exposed through signaling transactions provides useful network reconnaissance of targeted networks. Key functions such as user authentication, mobility management, SMS, voice, and data session management provide a detailed landscape of the core network hosts of each mobile operator. Moreover, the network responses to signaling transactions can reveal allow/block/respond rules configured in operator network firewalls.

Armed with this network visibility, actors can virtually probe network firewalls while remaining undetected, locating surface vulnerabilities and hosts to deploy backdoors and move laterally within operator core networks to relay C2 commands via the IPX. It can also facilitate the distribution of user device spyware via SS7-based SMS phishing lures and silent OTA messages.

Global Implications

Findings of China state-owned IPX and SS7 interconnect networks used by mobile operators in key regions raises significant security concerns. In Five Eyes intelligence partner New Zealand and South Korea, two mobile operators rely on China Mobile International for IPX services. The leading operators in Indonesia, Thailand, Malaysia, Vietnam, and Philippines all use China state-owned interconnect networks, representing significant points of exposure in Southeast Asia. Taiwan, a frequent target of PRC-linked telecom attacks in 2024 has an operator using China Mobile International and three mobile operators utilizing China-based CITIC Telecom International, a company tied to Chinese state interests.

Dependencies on mobile operators and their users passing internet and communications traffic through China's interconnect infrastructure reveal tools for state-sponsored surveillance. Unless addressed through policy intervention, the integration of these networks into global telecom infrastructure poses a direct threat to the privacy and security of billions of mobile users worldwide.

Expanding the Risk Surface: Huawei, ZTE, and Supply Chain Exposure

Recent U.S. government efforts to curtail the influence of Chinese telecom giants Huawei and ZTE brings attention to another national security concern: the convergence of mobile supply chain risks with mobile interconnect exposure.

Analysis of March 2025 IR.21 data submitted by mobile operators to the GSMA revealed 207 mobile operators in 144 countries that have deployed core network equipment manufactured by Huawei or ZTE. These deployments also show five rural mobile networks operating within the United States. Among them is Tampnet, a provider of maritime communications for offshore oil platforms, shipping lanes, and sea-based operations that lists Huawei as their HLR and MSC vendor – critical equipment that stores subscriber network and service information, location, call and SMS delivery.

This deeper integration of Chinese core network infrastructure into global operator networks amplifies surveillance risks when combined with China's interconnect signaling routes. In many cases, the same mobile operators using Chinese interconnect providers for roaming traffic have also deployed Huawei or ZTE equipment in their signaling core, creating an end-to-end visibility path that spans access, control, and transport layers of the mobile network stack.

This dual exposure undermines traditional compartmentalization strategies for threat mitigation. As noted in supply chain reviews by the U.S. and allied governments, vulnerabilities introduced through Huawei and ZTE components are particularly concerning when they interface with unencrypted signaling protocols, already shown to be exploitable by state-aligned threat groups operating within China's mobile ecosystem.

In regions where critical infrastructure or defense operations depend on commercial mobile networks – such as maritime, border security, or transportation sectors — the risks aren't just theoretical. They create a layered surveillance surface that could be used for covert monitoring, communications interception, service disruption, or data exfiltration during times of geopolitical tension or conflict.

Mitigation strategies must consider not just the mobility transit path, but the underlying vendors powering the functions of the network.

Operators Using China Interconnect

Analysis of mobile operator IR.21 data from November 2024 shows the following mobile operators using China interconnect services shown in the tables below.

China Mobile International (CMI) IPX Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
Cambodia	Smart Axiata Co., Ltd	Smart
Cambodia	Viettel (Cambodia) Pte., Ltd.	Metfone
China	China Mobile Limited	China Mobile
Fiji	Vodafone Fiji Pte Limited	Vodafone
Hong Kong, SAR	China Mobile Hong Kong Company	China Mobile
Hong Kong, SAR	SmarTone Mobile Communications	SmarTone
Indonesia	Indosat Ooredoo Hutchison	Indosat Ooredoo Hutchison
Indonesia	PT. XL Axiata	XL
Indonesia	PT. Smart Telecom	Smart Telecom
Japan	NTT Docomo, Inc.	NTT Docomo
Kazakhstan	Beeline Kazakhstan	Beeline
Kenya	Telkom Kenya Limited	Telkom
Laos	Star Telecom Company Limited	Unitel
Malaysia	Celcom Axiata Berhad	Axiata
Malaysia	DiGi Telecommunications Sdn Bhd	Digi
Malaysia	TM Technology Services Sdn. Bhd.	Unifi
Maldives	Dhiraagu	Dhiraagu
New Zealand	Spark New Zealand	Spark
New Zealand	Two Degrees Networks Limited	2 Degrees
Pakistan	CMPak Limited	Zong
Palau	Palau Mobile Communications Inc.	PMCI
Peru	Viettel Peru	Bitel
Philippines	Globe Telecom	Globe
Philippines	Smart Communications, Inc.	Smart
Russia	LLC T2 Mobile	Tele2
Russia	MegaFon PJSC	MegaFon
Russia	MIATEL LLC	MIATEL
Russia	PJSC Mobile TeleSystems (MTS)	MTS
Russia	VimpelCom PJSC	Beeline
Saudi Arabia	Etihad Etisalat Company	Mobily
Singapore	M1 Limited	M1
Singapore	StarHub Mobile Pte Ltd	StarHub
Slovenia	T-2 d.o.o.	T2
South Africa	Wireless Business Solutions (Pty)	Rain
South Korea	LG Uplus, Corp.	LG
South Korea	SK Telecom Co., Ltd.	SK Telecom
Sri Lanka	Dialog Axiata Plc	Airtel
Sri Lanka	Dialog Axiata Plc	Dialog
Taiwan	Far EasTone Telecommunications	Far EasTone
Thailand	Advanced Wireless Network Com-	AIS
Thailand	National Telecom Public Company	True Move
Thailand	True Move H Universal Communica-	True Move
Thailand	True Move H Universal Communica-	DTAC
Vietnam	Mobifone	Mobifone
Vietnam	Vietnamobile Telecommunications	Vietnamobile
Vietnam	Vinaphone	Vinaphone

China Mobile International (CMI) SS7 Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
China	China Mobile Limited	China Mobile
China	China Mobile Limited	China Mobile
Egypt	Orange Egypt for	Orange
Egypt	Vodafone Egypt	Vodafone
Hong Kong, SAR	China Mobile Hong Kong	China Mobile
Indonesia	PT. XL Axiata	XL
Kenya	Telkom Kenya Limited	Telkom
Malaysia	Celcom Axiata Berhad	Axiata
New Zealand	Two Degrees Networks Limited	2 Degrees
Pakistan	CMPak Limited	Zong
Palau	Palau Mobile Communications	PMCI
Palau	Palau Mobile Communications	PMCI
Philippines	Globe Telecom	Globe
Russia	MegaFon PJSC	MegaFon
Russia	VimpelCom PJSC	Beeline
Slovenia	T-2 d.o.o.	T2
South Africa	Wireless Business Solutions	Rain
Thailand	True Move H Universal	DTAC
United Arab Emirates	du	du

China Telecom Global IPX Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
China	China Telecommunications	China Telecom
Macau	China Telecom (Macau) Company	China Telecom
Philippines	DITO Telecommunity	Dito Telecommunity

China Unicom Global (CUG) IPX Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
China	China Unicom	China Unicom
Hong Kong, SAR	Hutchison Telecommunications Hong Kong Holdings Limited	Hutchison
Hong Kong, SAR	SmarTone Mobile	SmarTone

CITIC Telecom International IPX Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
Hong Kong, SAR	China Mobile Hong Kong Co. Ltd.	China Mobile
Hong Kong, SAR	Hutchison Telecommunications Hong Kong Holdings Limited	Hutchison
Hong Kong, SAR	SmarTone Mobile Communications	SmarTone
Indonesia	Indosat Ooredoo Hutchison	Indosat Ooredoo Hutchison
Philippines	Globe Telecom	Globe

CITIC Telecom International SS7 Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
Burundi	Viettel Burundi S.A.	Lumitel
China	China Mobile Limited	China Mobile
China	China Unicom	China Unicom
Hong Kong, SAR	China Mobile Hong Kong Co. Ltd.	China Mobile
Hong Kong, SAR	Hong Kong Telecommunications (HKT) Limited	CSL
Hong Kong, SAR	Hong Kong Telecommunications (HKT) Limited	PCCW
Hong Kong, SAR	Hutchison Telecommunications	Hutchison
Hong Kong, SAR	SmarTone Mobile Communications	SmarTone
Indonesia	PT. Smart Telecom	Smart Telecom
Japan	KDDI Corporation	KDDI
Macau	China Telecom (Macau) Company	China Telecom
Macau	CTMGSM	CTM
Macau	Hutchison Telephone (Macau) Company Limited	Hutchison
Macau	SmarTone Mobile Communications (Macau) Limited	SmartOne
Peru	Viettel Peru	Bitel
Philippines	Globe Telecom	Globe
Philippines	Smart Communications, Inc.	Smart
South Korea	SK Telecom Co., Ltd.	SK Telecom
Taiwan	Asia Pacific Telecom Co., Ltd. (APT)	Asia Pacific
Taiwan	Far EasTone Telecommunications	Far EasTone
Taiwan	Taiwan Mobile Co.Ltd	Taiwan Mobile
Thailand	Advanced Wireless Network	AIS
Thailand	True Move H Universal Communication Co., Ltd (THACA)	True Move
Timor-Leste	Viettel Timor Leste Unipessoal Lda	Telemor
Vietnam	Viettel Group	Viettel Mobile

PCCW Global Hong Kong IPX Customers

OPERATOR COUNTRY	ORGANIZATION NAME	MOBILE BRAN
Equatorial Guinea	Muni S.A.	Muni
Hong Kong, SAR	Hong Kong Telecommunications (HKT) Limited	CSL
Hong Kong, SAR	Hong Kong Telecommunications (HKT) Limited	PCCW
Liechtenstein	Telecom Liechtenstein AG	FLI
Saudi Arabia	MTC Saudi Arabia (Zain)	Zain
Thailand	Advanced Wireless Network Company Limited	AIS

About iVerify

iVerify Enterprise: Real Threats. Every Device.
iVerify is a pioneer in mobile endpoint detection and response (EDR) solutions, providing advanced protection against the real threats mobile devices face. The company's comprehensive security platform safeguards organizations from fileless malware, smishing, malicious applications, ransomware operations, and breaches resulting from credential theft. iVerify's solutions span from consumer to enterprise and government sectors, offering both privacy-focused BYOD protection and enterprise-grade security capabilities to ensure every device in the workplace is secure.

iVerify fundamentally differs from legacy mobile security products limited to signature-based threat detection and offers virtually no response capability. iVerify uses heuristic-based threat hunting to identify threats and infected devices, including the industry's most sophisticated Pegasus detection capability. This makes iVerify the only solution to offer a complete mobile EDR solution that detects threats and quickly responds to eliminate the impact of compromised BYOD and corporate-owned mobile devices across the enterprise, greatly reducing the likelihood of a corporate breach. This is why leading banks and government institutions use iVerify to protect their organizations.

iVerify also offers special protection at https://iverify.org/ for journalists and civil society.

Request a demo to experience our advanced features firsthand at iVerify.io.

Contributors

Gary Miller, Citizen Lab Senior Researcher & Founder of the Mobile Surveillance Monitor project (https://mobileintelligence.org)

Daniel Kelley, Threat Researcher

iVerify Threat Research Team

Get In Touch With Us

Request a demo of iVerify Mobile EDR solution at iverify.io/contact

iVerify.

www.iverify.io