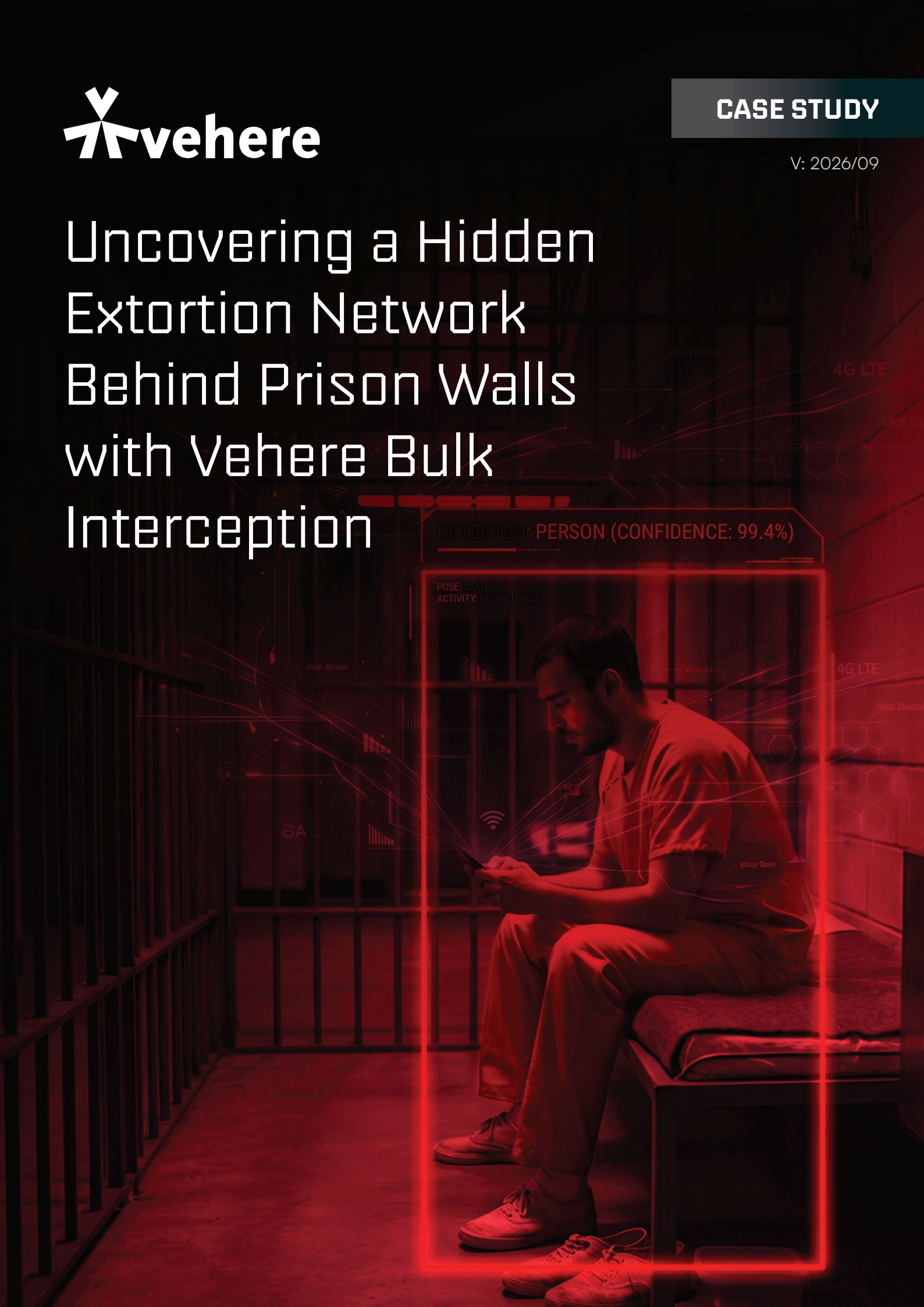
vehere

CASE STUDY

V: 2026/09

Uncovering a Hidden Extortion Network Behind Prison Walls with Vehere Bulk Interception



About the Customer

A Lawful Enforcement Agency (LEA) operating across a sensitive border region needed deeper visibility into unauthorized mobile communications and hidden identities linked to organized criminal networks.

The agency was investigating an incarcerated gang leader suspected of directing an extortion network from inside a high-security correctional facility, communicating with associates within and beyond the border region through unauthorized mobile devices. Frequent SIM and handset changes made it difficult to maintain a persistent view of the communication trail.

The agency deployed Vehere Bulk Interception Monitoring Center (BIMC) to process high-volume intercepted communications and correlate identities, devices, locations, and communication links, turning fragmented communication activity into actionable network intelligence.

> ***The challenge was not simply intercepting communications. We needed to identify the devices, numbers, locations, and relationships hidden within large volumes of communication data and connect them back to the individuals and networks under investigation.***

The Growing Threat Landscape

Criminal networks increasingly exploit mobile communications to change devices, rotate subscriber identities, and operate across geographic boundaries, making it harder for Lawful Enforcement Agencies (LEAs) to maintain continuity of intelligence.

The scale of the challenge is significant. In 2024, analysis by Ministry of Home Affairs and State Force identified 28,200 mobile handsets misused in cybercrime, with 20 lakh mobile numbers found to have been used with those handsets.*

The challenge has continued to grow. As of July 15, 2026, the Department of Telecommunications reported that its ASTR AI and big-data analytics system had identified more than 88 lakh suspicious mobile connections that were subsequently disconnected after failing reverification.**

For LEAs operating across sensitive border environments, the challenge is therefore not simply intercepting communications; it is extracting intelligence from high-volume communication data and connecting fragmented identities. Correlating MSISDNs, IMEIs, locations, communication activity, and historical relationships can help investigators move from an isolated device or number to the individuals, relationships, and networks operating behind them.

Challenges Faced

- **Dynamic Subscriber:** Device Associations: Frequent MSISDN—IMEI changes fragmented target profiles and disrupted continuity of communication intelligence.
- **Fragmented Communication Identities:** Multiple MSISDNs, SIMs, and devices obscured the persistent identity of the individual behind the communication.
- **Unauthorized Device Activity:** Unknown devices operating within sensitive or restricted locations created blind spots in mobile activity monitoring.
- **Insufficient Historical Context:** New identifiers and communication events lacked the historical associations required to distinguish legitimate changes from deliberate identity concealment.
- **High-Volume Correlation Complexity:** Correlating subscribers, device, communication, location, and historical data across large datasets was difficult through manual analysis.
- **Hidden Network Relationships:** Newly discovered numbers and devices lack an obvious connection to known entities, making multi-hop communication and association analysis critical to exposing the wider network.

**Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2020197&noshow=1*

***(Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2288303&lang=1&reg=1)*

Vehere Solution

The Agency deployed Vehere Bulk Interception Monitoring Center (BIMC) to transform high-volume intercepted communications into continuous identity, location, and relationship intelligence. From One Device Change to a Network Lead

The deployment included:

High-Volume Data Ingestion: Processes intercepted communication and signaling data at scale within a unified intelligence environment.

Continuous Identity Correlation: Correlates MSISDN, IMEI, location, and communication activity to maintain persistent identity relationships.

Automated Phone-Swap Detection: Detects deviations in established MSISDN-IMEI relationships and generates Phone Swap Activity Alerts.

Actionable Intelligence Alerts: Transforms multi-dimensional correlations into prioritized investigative leads, enabling analysts to focus on high-value activity.

Alternate Number Discovery: Pivots from known devices and identities to identify previously unknown MSISDNs associated with the communication footprint.

Historical Intelligence Correlation: Correlates new identifiers with past communications, devices, locations, and known entities to establish an investigative context.

Location and Communication Link Analysis: Connects devices, numbers, locations, and communication relationships to uncover hidden links and suspicious activity within sensitive areas.

How Vehere Bulk Interception Monitoring Center (BIMC) Delivers Intelligence

From Intercepted Data to Investigative Intelligence

Data Sources

Mobile Networks:	VoIP and VoWiFi:	Voice and SMS:	Data Services:	Signaling:
2G / 3G / 4G / 5G	SIP, RTP, Signaling	Voice, SMS, USSD	IPDR, GTP, HTTP, Data	SS7 / Diameter / SIP / IMS

Vehere Bulk Interception Monitoring Center (BIMC)

High-Volume Interception and Communications Intelligence Platform

1 Bulk Data Ingestion and Normalization
- High-volume ingestion of intercepted communication and signaling data.
- De-duplication and validation.
- Normalize and standardize into unified schema.
- High-throughput processing pipeline.

2 Identity Correlation Engine
- Correlate MSISDN, IMEI, IMSI, IP, Location and Time.
- Builds persistent identity graph.
- Maintains historical relationships and communication patterns.

3 Anomaly Detection (Phone Swap)
- Detect deviations in MSISDN-IMEI relationships.
- Identify new IMEI for known MSISDN or known IMEI with new MSISDN.
- Configurable detection rules and thresholds.

4 Intelligence Enrichment and Pivoting
- Pivot from device to alternate MSISDNs.
- Identify associated devices, locations and entities.
- Correlate historical communications and behavior.

5 Alert Generation and Prioritization
- Generate contextual intelligence alerts.
- Risk score and priority assignment.
- Minimize noise, maximize analyst focus.

6 Investigator Action
- Review alerts and correlated insights.
- Visualize links and patterns.
- Drill down and take investigative action.
- Export and share intelligence.

> *Vehere BIMC enabled us to connect seemingly isolated devices and communication changes into a broader intelligence picture. This helped us identify unauthorized devices, uncover alternate communication identities, and trace relationships across the network.*

Outcomes Delivered

Following deployment, the agency strengthened its ability to extract actionable intelligence from high-volume intercepted communications, even as subscribers, devices, and communication identities changed.

Persistent Communication Visibility: Maintained intelligence continuity across changing MSISDNs, IMEIs, SIMs, and handsets.

Automated Identity Change Detection: Automatically surfaced new MSISDN - IMEI associations, eliminating manual comparison of historical records.

Context-Rich Intelligence: Correlated identity, device, communication, location, and historical data to distinguish isolated events from meaningful patterns.

Expanded Network Intelligence: Connected newly identified identities with known targets, associates, devices, and communication relationships.

Hidden Identity Discovery: Exposed alternate numbers and previously unknown devices associated with established communication identities.

Faster Investigative Action: Converted high-volume intercepted data into prioritized intelligence leads, enabling investigators to move from a single device anomaly to a broader communication network with less manual analysis.

From Changing Numbers to Persistent Identity Intelligence

Vehere Bulk Interception helped the Agency move beyond monitoring known numbers to understanding the changing communication identities behind them - giving investigators the intelligence needed to detect unauthorized devices, uncover alternate numbers, and map the communication networks supporting organized criminal activity.

About Vehere

Vehere is an AI cyber defense company operating at the intersection of national security and enterprise security. Our AI-powered Network Intelligence platform processes petabytes of network data at terabit speed, empowering government agencies with real-time intelligence, advanced analytics, and actionable insights. From preventing emerging threats to accelerating investigations, Vehere helps governments and law enforcement agencies protect national sovereignty and strengthen public safety.

Address:
1390 Market Street
Suite 200, San Francisco, CA 94102

Unit No. 5, 1st Floor, Andaz, Asset Area 1
Aerocity, New Delhi-110037

E: sales@vehere.com

W: www.vehere.com