RIDGELINE INTERNATIONAL

# Mitigating Ubiquitous Technical Surveillance (UTS) Risks in Large Scale Combat Operations (LSCO)

## *Mitigating Risks in High-Threat Environments*

*October 2025*

# Table of Contents



# Executive Summary

INDOPACOM personnel face an immediate and escalating threat from Ubiquitous Technical Surveillance (UTS) that fundamentally compromises our ability to maintain operational surprise in Large Scale Combat Operations (LSCO).

The digital surveillance economy systematically collects, resells, and analyzes our personnel's commercial transactions and digital behaviors, creating a comprehensive intelligence picture available to our adversaries. This commercial data ecosystem converges with state-sponsored intelligence collection activities that specifically target the INDOPACOM Area of Responsibility (AOR), generating unprecedented vulnerabilities during our most critical operational phases—training, planning, and initial movements.

The proliferation of sensor-rich mobile devices, open-source data aggregation, and the digital surveillance economy which collects and analyzes personal and operational data has fundamentally shifted the intelligence advantage to our adversaries. They can now anticipate our actions, influence our operations, and circumvent traditional force protection measures by exploiting data streams that did not exist a decade ago. Critically, our adversaries operate without the legal, regulatory, and ethical constraints that govern US intelligence activities, providing them asymmetric advantages in data collection and exploitation.

> *Traditional operational security measures, designed for an analog era, are insufficient against adversaries who leverage the global digital surveillance infrastructure. The threat is not theoretical—it is actively compromising our operational effectiveness today.*

# The Problem

The movement associated with Large Scale Combat Operations (LSCO) is inherently difficult to conceal. However, initial low-level movements prior to real-world operations, as well as during training exercises and advanced planning events, are particularly vulnerable to UTS threats. This exposure can significantly compromise operational security, allowing adversaries to anticipate and counter unit actions effectively.

However, Ridgeline’s tech-enhanced training and technology solutions for digital signature management provides personnel with the practical knowledge, tools, and skills with hands-on instruction to manage UTS threats.

## INDOPACOM-Specific Threat Environment

### *Digital Surveillance Economy Exploitation*

- Commercial data brokers selling location and behavioral data to foreign entities
- Credit card and financial transaction pattern analysis revealing deployment preparations
- Travel booking and logistics data aggregation exposing movement patterns
- Consumer app data harvesting from military and personnel devices

### *Adversarial State Collection Activities*

- Systematic collection of US personnel data through commercial channels
- Targeted exploitation of INDOPACOM personnel social media and digital footprints
- Strategic investment in regional telecommunications and technology infrastructure
- Coordinated collection operations targeting military families and contractors

### *Regional AOR Vulnerabilities*

- High-density sensor environments in allied urban areas
- Adversary-controlled or influenced telecommunications infrastructure
- Commercial technology with embedded collection capabilities
- Regional data localization laws facilitating foreign intelligence access

# Current Landscape

Historically, high-quality targeting data and widespread surveillance has been limited to well-resourced state actors. However, the increasingly universal availability of emerging and disruptive technologies has allowed lesser combatants to utilize commercial technologies and data to find, fix, and finish high-value targets. For example, Ukraine has had great success finding, targeting, and destroying Russian forces based on Russian soldiers' unauthorized cell phone signals, including a rocket attack on a Russian barracks that killed 63 personnel.[1]

Additionally, adversaries with previously limited command, control, computing, communications, cyber, intelligence, surveillance, reconnaissance and targeting capabilities and capacity will utilize commercial-off-the-shelf technologies, publicly available data, and open-source artificial intelligence/ machine learning applications and expertise to achieve relative parity with the United States.[2]

[1] *The Operational Environment 2024-2034: Large-Scale Combat Operations*, Department of the Army Headquarters, United States Army Training and Doctrine Command.
[2] *The Operational Environment 2024-2034: Large-Scale Combat Operations*, Department of the Army Headquarters, United States Army Training and Doctrine Command.

# Ridgeline's Solution Framework

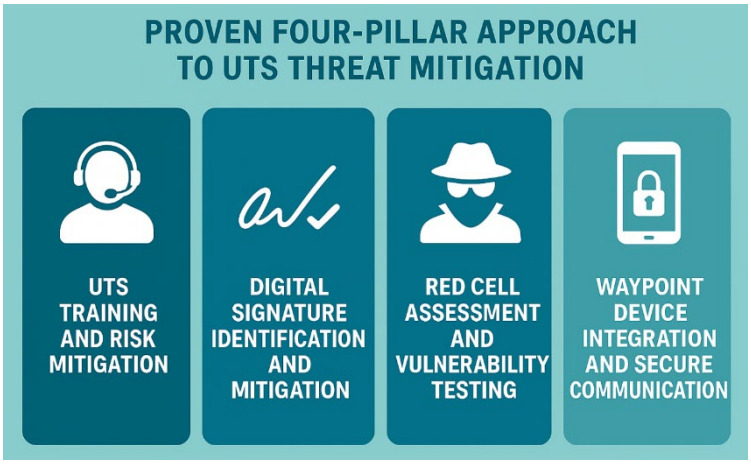
Based on our successful implementations within the USIC and DoD communities, we have developed a proven four-pillar approach to UTS threat mitigation:

## Pillar 1: UTS Training and Risk Mitigation

**Objective**: Educate and prepare personnel to reduce technical signatures and minimize data collection vulnerability.

*Implementation:*

- Customized training programs tailored to unit-specific operational requirements
- Risk assessment protocols for identifying individual and unit-level vulnerabilities
- Behavioral modification techniques to reduce digital footprint during sensitive operations
- Continuous education on emerging UTS threats and countermeasures




## Pillar 2: Digital Signature Identification and Mitigation

**Objective**: Employ advanced analytics to identify and neutralize data collection during exercises and operations.

*Implementation:*

- Real-time digital signature analysis during training and operational phases
- Commercial AdWare detection and mitigation protocols
- Cell phone signature masking and alternative communication methods
- Comprehensive technical data pattern analysis to prevent movement prediction

## Pillar 3: Red Cell Assessment and Vulnerability Testing

**Objective**: Conduct adversarial assessment of current UTS mitigation capabilities and provide actionable improvements.

*Implementation:*

- Comprehensive "Red Cell" evaluation using adversarial collection methodologies
- Unit-specific vulnerability assessments across digital, technical, and behavioral domains
- Actionable recommendation development with prioritized implementation timelines
- Follow-up assessments to measure improvement and identify residual risks

### Pillar 4: Waypoint Device Integration and Secure Communication

**Objective**: Provide secure communication capabilities and establish data activity baselines for continuous assessment.

*Implementation:*

- Waypoint device deployment for secure, UTS-resistant communication
- Baseline establishment for normal vs. operational data activity patterns
- Continuous monitoring throughout planning and execution phases
- Secure alternative communication networks independent of commercial infrastructure

# Conclusion & Ridgeline Profile

Modern LSCO will be a competition between the hiders and the finders, with only fleeting exploitation opportunities for both. If a target can be seen, it can be killed. The ability of the operators to protect themselves on this transparent battlefield will be paramount to their survival and success. The ability to hide in plain sight takes on even greater importance with the mass and precision of modern weapons systems, especially in the Indo-Pacific theater.

Ridgeline organizes our products into three key disciplines: understanding the threat, controlling the flow of data, and shaping the narrative about your activities. Applying this comprehensive approach allows you to avoid investigative triggers, prevent forensic reconstruction, and protect your operations.

# Call to Action

Ridgeline is laser-focused on solving our customers' toughest data challenges. Data collection and technical surveillance are complex, ever-evolving problems. Our solutions tackle this complexity by spanning not just digital privacy, cybersecurity, data analysis, or tech integration, but all of these combined and more. **We're constantly iterating to improve our offerings and stay ahead of the threat. *Are you?***

# Get In Touch

David Huisenga
Senior Growth Advisor
C: 571-247-1086
E: dhuisenga@ridgelineintl.com
www.ridgelineintl.com
Ridgeline International, LLC.