C O N F I D E N T I A L P R O P O S A L

NATIONAL RF INTRUSION DETECTION SYSTEM

FOR SOUTH AFRICAN MINING OPERATIONS

A Proposal for Strategic Partnership

Submitted to: Minerals Council South Africa | Strategic Security Partners

Date	April 2026
Classification	CONFIDENTIAL — For Authorised Recipients Only
Prepared By	Kyle — Mining Security Technology Initiative
Contact	Available upon request
Version	1.0 — Initial Concept Proposal

1. Executive Summary

South Africa's mining sector faces an escalating threat from illegal intrusion, contraband communication devices, and organised criminal syndicates — including illegal artisanal miners (zama zamas) — operating across vast, difficult-to-monitor terrain. Existing physical security measures are costly, labour-intensive, and often insufficient given the scale of operations.

This proposal outlines a scalable, technology-driven National RF Intrusion Detection System capable of passively detecting unauthorised electronic devices — including cellular phones, two-way radios, and wireless communication equipment — across mine properties of up to 10,000 hectares and beyond.

The system leverages proven open-source RF detection technology, LoRa mesh networking, GPS geolocation, and satellite uplink infrastructure to deliver real-time alerts to centralised security command centres. The architecture is designed to scale from a single mine site to a nationally unified mining security network.

We seek strategic partnership with the Minerals Council South Africa, international security technology firms, and relevant government bodies to develop, pilot, and commercialise this system.

2. The Problem

2.1 Scale of the Threat

South African mines collectively span millions of hectares and represent critical national infrastructure. The threats faced include:

- Illegal mining syndicates (zama zamas) operating underground and in restricted surface areas
- Contraband cellular devices used to coordinate theft, sabotage, and illegal entry
- Insider threats facilitated by covert communication devices
- Real-time coordination between criminal elements using unauthorised RF-emitting devices
- Traditional perimeter security failing to detect intrusions across vast, irregular terrain

2.2 Why Existing Solutions Fall Short

Current approaches — physical patrols, CCTV, and perimeter fencing — suffer from significant limitations:

- 10,000+ hectare properties make physical patrol coverage impractical and expensive
- CCTV requires line-of-sight and dense infrastructure investment
- Criminals routinely exploit terrain to evade visual detection

- No existing unified system provides real-time RF device detection at mine scale in South Africa

3. Proposed Solution

3.1 System Overview

The National RF Intrusion Detection System (NRIDS) is a layered, passive detection network that identifies the RF emissions produced by any active electronic device — without intercepting communications content — and geolocates the source with sufficient precision to direct a security response.

Key principle: Any mobile phone, even on silent, continuously emits detectable radio frequency signals including WiFi probe requests, Bluetooth advertising packets, and GSM/LTE network heartbeats. These emissions cannot be disabled by the user without powering off the device entirely.

3.2 System Architecture

Layer	Component	Function
Detection Node	SDR receiver + WiFi/BT scanner + GPS module	Passively detects RF emissions; timestamps and geotags each event
Local Mesh	LoRa radio network	Relays detection events from nodes to gateway without cellular dependency
Edge Gateway	uConsole Linux terminal (ClockworkPi)	Aggregates node data; runs analysis; manages local alerts and uplink
Satellite Uplink	Swarm / Astrocast / Iridium SBD	Transmits alerts from remote sites to national command platform
National Platform	Cloud-based security dashboard	Unified map view of all detections; alert routing; pattern analysis
Response Layer	Mine security control room / rapid response teams	Receives geolocated alerts; dispatches physical response

3.3 RF Detection Capabilities

Each detection node passively monitors the following emission types:

- GSM / LTE — cellular heartbeat signals to base stations (850MHz, 900MHz, 1800MHz, 2100MHz)
- WiFi (2.4GHz / 5GHz) — probe requests broadcast by any WiFi-enabled device
- Bluetooth / BLE (2.4GHz) — advertising packets broadcast continuously by most smartphones
- Sub-GHz (433MHz / 868MHz) — two-way radios, walkie-talkies, and remote devices

No call interception or content monitoring occurs. The system detects the presence of an emitting device only — fully compliant with RICA (Regulation of Interception of Communications Act) passive monitoring provisions.

3.4 Geolocation Method

Precise device location is achieved through Time Difference of Arrival (TDoA) triangulation using a minimum of three detection nodes within range of the target emission. Combined with GPS-stamped node positions, the system can resolve device location to within 10–50 metres depending on node density and terrain.

---

4. National Satellite Integration

4.1 The Scale Challenge

South Africa's mining operations span some of the most remote and RF-infrastructure-sparse terrain on the continent. Traditional cellular or fibre backhaul is unavailable or cost-prohibitive across many operational areas. Satellite integration solves this definitively.

4.2 Recommended Satellite Platforms

Platform	Strengths	Best Use
Swarm (SpaceX)	Low cost, global LEO coverage, compact hardware	High-volume detection event uplink from remote nodes
Astrocast	Purpose-built for IoT sensor networks, low power	Always-on remote monitoring nodes
Iridium SBD	Proven, reliable, SA mining industry trusted	Mission-critical alert uplink with guaranteed delivery
HawkEye 360	Satellite-based RF detection from orbit	National-scale RF anomaly mapping; complements ground network

4.3 National Intelligence Value

A satellite-connected national network transforms individual mine site security into a unified national intelligence asset:

- Cross-property pattern detection — tracking devices that appear at multiple mines
- Temporal analysis — identifying coordinated intrusion timing across sites
- Syndicate mapping — building RF device signature databases linked to criminal intelligence
- Integration potential with SAPS Crime Intelligence and Minerals Council security structures

---

5. Legal and Regulatory Framework

The system is designed to operate within South African law. Critical distinctions:

PERMITTED — Passive Detection	NOT APPLICABLE — Not Performed
Detecting that an RF-emitting device is present	Intercepting call or message content
Geolocating emission source via signal triangulation	Identifying subscriber identity (IMSI/IMEI capture)
Logging detection timestamps and coordinates	Jamming or disrupting communications
Alerting security personnel to unauthorised device presence	Any active interference with device operation

Legal counsel specialising in RICA and ICASA regulations should be engaged during the pilot phase to confirm operational parameters. Mine site deployment on private property with appropriate signage and employee disclosure strengthens the legal position substantially.

6. Partnership Opportunity

6.1 What We Bring

- Conceptual architecture and system design for the NRIDS platform
- Knowledge of applicable RF detection hardware and open-source tooling
- Understanding of the South African mining security landscape
- Commitment to developing a commercially viable, scalable product

6.2 What We Seek

- Minerals Council South Africa — pilot site access, industry endorsement, co-funding
- CSIR — engineering partnership for prototype development and testing
- Israeli defence-commercial partners (e.g. Elbit Systems, Rafael Commercial) — advanced RF sensor technology and systems integration expertise
- Satellite IoT providers — commercial partnership for network connectivity
- SAPS Crime Intelligence / SSA — operational integration framework for national intelligence sharing
- Private equity / venture capital — commercialisation funding for national rollout

6.3 Proposed Pilot

We propose a structured three-phase pilot programme:

Phase	Duration	Objectives

Phase 1 — Proof of Concept	3 months	Deploy 5–10 detection nodes on a single willing mine site. Validate detection range, geolocation accuracy, and LoRa mesh performance. Establish baseline metrics.
Phase 2 — Pilot Scale-Up	6 months	Expand to full site coverage (10,000 Ha). Integrate satellite uplink. Connect to command dashboard. Measure security incident reduction vs baseline.
Phase 3 — National Rollout	12–24 months	Deploy to 5+ mining operations. Launch national command centre. Establish cross-site intelligence sharing. Commercialise as managed security service.

7. Commercial Model

7.1 Revenue Streams

- Hardware supply — detection node kits supplied to mine operators
- Managed Security Service (MSS) — monthly subscription per site for monitoring, maintenance, and alerting
- National intelligence platform — tiered access for industry bodies and law enforcement
- International licensing — exportable model for mining operations across Africa and globally

7.2 Market Scale

South Africa has approximately 1,500 active mining operations. Even conservative penetration of 10% of mid-to-large operations represents a substantial recurring revenue base. The model is directly exportable to DRC, Zambia, Zimbabwe, Ghana, and other major African mining jurisdictions facing identical illegal mining challenges.

8. Proposed Next Steps

We invite interested parties to engage on the following basis:

- Initial confidential briefing meeting to present technical proof of concept
- Site visit to a willing mining operation to assess detection requirements
- MOU / NDA execution to protect all parties during evaluation
- Joint working group formation: technical, legal, and commercial workstreams
- Phase 1 funding agreement and pilot site identification

9. Closing Statement

Illegal mining and organised crime cost the South African mining industry billions of rands annually — in direct theft, infrastructure damage, safety incidents, and legal liability. The technology to detect, locate, and deter these threats exists today. What is required is the will to deploy it systematically and at scale.

This proposal represents a viable, lawful, and commercially sustainable path to transforming mine site security from reactive physical patrol to proactive, intelligence-driven RF detection — nationally unified and satellite-connected.

We look forward to discussing this opportunity with the right partners.