White Paper

Phantom Zero: ECHO I – Command the Invisible

Company: Phantom Zero

Device: Echo I

Executive Summary

Welcome to a new era of digital dominance. Echo I by Phantom Zero is not merely a tool—it is a field command center disguised as a compact, rugged device. Built for cyber warfare specialists, ethical hackers, embedded developers, and wireless engineers, Echo I consolidates an arsenal of capabilities into a seamless and secure platform. With its hybrid processing engine, wide-spectrum SDR, multi-protocol support, encrypted storage, and tactical-grade build quality, Echo I enables users to command digital and physical interfaces like never before.

When you hold Echo I, you're not troubleshooting networks—you're commanding them. You're not testing locks—you're unlocking possibilities. You're not decoding signals—you are the signal.

1. Introduction

Today's wireless and embedded environments are complex, fragmented, and increasingly adversarial. The demand for real-time, mobile-ready tools that operate across RF, NFC, BLE, Zigbee, IR, GPS, GPIO, and environmental sensing has never been higher. Echo I was designed from the ground up to provide this capability in a form factor that grants complete control in any terrain—urban, industrial, or remote.

Every inch of this device is designed to empower. From the dual-core processor architecture to the hardened casing, from the multi-protocol SDR to the onboard encryption chip, Echo I is not a device you use—it is a system you command.

2. System Architecture: Command Through Integration

2.1 Core Processor & Co-Processor

NXP i.MX RT1176DVMAA: This 1GHz Cortex-M7 with an auxiliary 400MHz Cortex-M4 forms the strategic brain of Echo I. Designed for real-time execution and deep signal analysis, this MCU tackles SDR, GPIO, and cryptographic tasks without hesitation.

ESP32-C6: Operating in parallel, this co-processor offloads network and short-range wireless communications (Wi-Fi 6, Bluetooth 5.3, Zigbee, Thread).

Control Impact: By separating communication from core logic, the device ensures uninterrupted analysis, live manipulation, and reactive behavior under high loads—making it ideal for real-time hacking, spoofing, and rapid protocol response.

2.2 Radio & Communication Modules

Analog Devices AD9361 SDR: With full-spectrum access from 70 MHz to 6 GHz, this chip empowers Echo I to capture, analyze, and emit almost any signal—public, private, encrypted, or proprietary.

ST25R3916 NFC + EM4095 RFID: Full-frequency support for high-frequency (13.56 MHz) and low-frequency (125 kHz) RFID. Execute emulation, eavesdropping, cloning, or fuzzing with ease.

u.FL/SMA Ports: Connect directional or omni antennas on the fly. Adapt range, stealth, or power to your situation.

Control Impact: You gain the power to listen, interrupt, or imitate virtually any wireless protocol—from smart locks and industrial tags to car fobs and building access systems.

2.3 Expansion & I/O

USB-C OTG + PD: Attach payloads, power banks, HID injectors, or firmware targets.

Qwiic I²C and GPIO Header: Seamlessly plug in sensors, logic controllers, or external triggers with no soldering required.

MCP23017: Expands your interface with 16 additional I/O pins.

Control Impact: Whether interfacing with industrial machinery or microcontrollers, you’re prepared to react and reprogram in seconds.

2.4 Display & Human Interface

2.4” IPS LCD: Real-time visuals with vibrant color, backed by an optional capacitive touchscreen.

Rotary Encoder & D-Pad: Navigate and deploy scripts, protocols, or payloads with military precision.

Multisensory Feedback: RGB LED, buzzer, haptics—designed for stealth or alert depending on your environment.

Control Impact: Whether in silent mode during covert ops or full feedback for field debugging, Echo I adapts to your presence, not the other way around.

2.5 Battery & Power System

5000mAh Li-Po Battery: Full-day deployment capability.

Advanced PMICs: Intelligent charging with thermal protection, multi-rail power management, and USB PD support.

Thermal System: Copper pipes, graphite pads, and low-profile aluminum heat sinks keep you operational during extended SDR sessions or ambient high heat.

Control Impact: Whether performing signal injection in a 100°F rooftop operation or GPS spoofing in an underground carpark, Echo I remains cool, quiet, and reliable.

2.6 Infrared & Sensor Suite

10W IR LED + High-Gain Receiver: Transmit or hijack remote signals from 20+ feet. Break IR-based access controls or automate consumer IR interfaces.

DFRobot 10-DOF IMU: Tracks motion, tilt, pressure, altitude.

BME280, BH1750, A3144: Temperature, humidity, barometric pressure, ambient light, and magnetic field sensing.

Control Impact: Build logic-based automation or intrusion triggers based on your physical surroundings. Program environmental reactions or deploy in drones and bots.

2.7 Security & Storage

ATECC608A: Secure enclave for encrypted key storage, anti-cloning measures, and authentication.

eMMC Flash + microSD: Store encrypted payloads, logs, configs, exploit chains, or field tools—inside or outside the device.

Control Impact: You are the gatekeeper. Your payloads are tamper-proof. Your traces are disposable.

2.8 Developer-First Access

CMSIS-DAP + JTAG/SWD Headers: Native development, debugging, and recovery from any failure or soft brick.

Safe Mode + Panic Wipe: Instantly protect your mission or identity.

Control Impact: Recover, reload, redeploy. No gatekeepers. No cloud dependencies. All power is local.

2.9 Rugged Tactical Build

Aluminum/Polycarbonate Shell: Drop-resistant.

Gorilla Glass: Scratch-proof, impact-tested.

Sealed USB/SD Ports: Protected from dust, rain, and impact.

Control Impact: Carry Echo I through rain, snow, sand, or sweat—it will survive.

3. Command Applications

Red Team Ops: Execute lock bypass, SDR jamming, access emulation, data injection, or physical automation.

Wi-Fi/BLE/Zigbee Analysis: Deploy fake APs, intercept smart devices, scan for vulnerabilities.

SDR Powerhouse: Tune into any radio communication, replay or manipulate data, inject false GPS, disrupt remote protocols.

USB Payload Deployments: Plug into systems and automate keystrokes, inject command sequences, deploy exfiltration payloads.

Education & R&D: Learn protocol internals, visualize data, run simulations, or test cryptographic limits in controlled labs.

Surveillance & Intelligence: Record environmental, location, and RF data over days—quietly and securely.

4. Competitive Advantage

Echo I has no equal. Others offer pieces: a SDR here, a Wi-Fi tool there, an NFC emulator somewhere else. Only Echo I combines all vectors—signal, physical, protocol, and software—into a single control device.

You do not connect to Echo I. You operate through it.

It is not a kit. It is a command platform.

It is not hackable. It is the hack.

5. The Road Ahead

Echo I is just the beginning. Our modular roadmap includes:

AI-augmented signal interpretation

Quantum-resistant payload vaults

Modular RF attack packs

Phantom OS – hardened, real-time, operator-optimized OS

6. Conclusion

Echo I puts power back where it belongs—in your hands. It is not just a tool for hackers or security professionals. It is for those who believe in absolute control, tactical precision, and unfiltered access to the digital and physical world.

This isn’t ownership. It’s dominion.

Contact: Phantom Zero Team
Email: info@phantomzero.org
Website: www.phantomzero.org