MetaMesh Wardriving SWAT Swarm

Introduction and Operational Need

Modern conflicts have revealed that **electromagnetic signals can swiftly betray unit positions**, enabling adversaries to target forces within minutes of detecting their radio emissions. U.S. Special Operations Forces (SOF) often operate in communications-denied, GPS-jammed environments where identifying and countering enemy communication nodes is paramount. The SBIR topic "Secure and Protect Infrastructure through Cyber-threat Emulation (SPICE)" seeks innovative ways to **emulate and counter cyber/EW threats** to protect friendly infrastructure. Our strategy addresses this by deploying a swarm of autonomous micro-drones and field "anchors" to *triangulate hostile communications and jamming sources*, then **actively disrupt and deceive enemy networks**. This approach combines *situational awareness, offensive electromagnetic warfare (EMW), and cyber deception* into a unified system. It fills a critical SOF capability gap: providing **real-time mapping of enemy signals and agile electronic attack**, all integrated into the ATAK/Blue-Force Tracker tactical network for command-and-control (C2).

Proposed Solution Overview

Our solution – tentatively called the **SWAT Swarm** (Spectrum Warfare Autonomous Triangulation Swarm) – comprises: **(1) a UAV-based signal scouting swarm**, and **(2) smart EMW anchor nodes**. The **micro-UAVs** (unmanned aerial vehicles) autonomously scout for RF emissions, while the **anchors** extend the network and conduct offensive EW (jamming and decoy operations). **ATAK** (Android Tactical Awareness Kit) serves as the C2 backbone for monitoring and directing these assets, effectively turning the system into a *mobile sensor and jammer network* that feeds data to the broader friendly force picture. By leveraging ATAK – which is "first and foremost, a kind of 'blue force tracker'" for team situational awareness – our solution ensures seamless integration with existing SOF digital infrastructure and the **Blue Force Tracking (BFT)** network. The following sections detail the technical approach and how it meets SPICE objectives.

UAV Swarm for Signal Triangulation

We deploy a **pack of lightweight drones (<<250g each)** equipped with software-defined radios (SDRs) and onboard AI. Acting as "flying network scouts," the drones perform an aerial form of wardriving – passively scanning for any RF signals (e.g. enemy tactical radios, cell uplinks, Wi-Fi) as they navigate through the battlespace. Upon detecting a signal of interest, the swarm collaborates to **classify the signal and estimate its location**. Each drone's onboard AI classifies emitter type in real time (e.g. distinguishing a Wi-Fi router vs. VHF radio) and filters out noise. Drones share detection data via a **decentralized Ultra-Wideband (UWB) mesh network** formed among themselves and the anchor nodes. Using UWB ranging (time-of-flight measurements) between drones and anchors, the system can pinpoint the emitter's relative location with sub-meter accuracy even in GPS-denied conditions. In effect, **multiple drones triangulate the source** by comparing signal strength/direction and precise inter-drone distances. This technique is analogous to how law enforcement IMSI-catcher systems triangulate phone signals, but here it's done with swarming drones for any RF source.

Once a drone localizes a hostile transmitter or jammer, it immediately **drops a geotagged "contact report" into the tactical network**. The contact report (containing emitter type and coordinates) is formatted as a standard Cursor-on-Target (CoT) message and broadcast through the UWB mesh to a team tablet or handheld device running ATAK. Through ATAK's network, this information is shared with all friendly units, populating their maps with icons for "enemy emitter at location X" in near-real time. In essence, the swarm turns scattered RF clues into actionable targets on the **Common Operational Picture (COP)**. This **persistent ISR (intelligence, surveillance, reconnaissance)** capability operates *organically and autonomously*, freeing operators from manual signal hunting. It directly supports the SPICE objective of **cyber-threat emulation** by detecting and mapping adversary network infrastructure – effectively *emulating a cyber/EW red team* that can find the weak links in communications. Moreover, by **triangulating enemy jammers**, the system not only protects our own comms but also enables rapid neutralization of those jamming sources (e.g. via airstrike or electronic counter-attack).

Technical Highlights – UAV Swarm:

Autonomous Micro-Drones: Small quadcopters (~250g) carrying SDRs and lightweight processors perform autonomous indoor/outdoor flight. Each has ~15–20 minute flight endurance and an onboard **neural network** optimized for RF signal classification. They navigate without GPS by using inertial sensors and peer-to-peer ranging (allowing operation "inside" buildings, caves, or urban canyons where GPS is denied).

UWB Mesh Network: Drones and anchors form a self-healing UWB mesh (IEEE 802.15.4z-class radios) for data relay and ranging. UWB was chosen for its low probability of intercept and resistance to jamming (wideband

signals raise the enemy's noise floor). The mesh lets the swarm operate beyond line-of-sight from the operator and maintain comms even underground or in cluttered environments. Each drone also serves as a node in this mesh, forwarding packets for peers.

Collaborative Geolocation: When a signal is detected, multiple drones share sensing data to fix its position. For example, **Time Difference of Arrival (TDOA)** techniques across the UWB network nodes allow precise triangulation of a radio emitter's location. The **anchor nodes** dropped by drones act as fixed reference beacons to improve localization accuracy and network range. By networking their measurements, the swarm effectively creates a **moving multi-static sensor array** that **self-localizes without GPS** and geolocates emitters with high confidence.

ATAK Integration: A small gateway device (could be a UWB-to-IP radio or a drone acting as gateway) connects the UWB mesh to an **ATAK End User Device** carried by the team. Detected emitter data is converted to CoT format, which ATAK (and by extension the **Blue Force Tracker network**) can ingest. ATAK essentially treats each detected signal as a "blue force" icon (or hostile icon) on the map, since ATAK is designed to track entities geospatially. This integration means our swarm's findings are instantly visible to any friendly with access to the tactical network, enabling coordinated action.

In summary, the UAV swarm gives SOF **unprecedented situational awareness of the electromagnetic spectrum** in denied areas – *Who is out there emitting, and where?* The approach is **feasible** with today's technology: for instance, palm-sized drones with low-power SDRs and AI have been demonstrated (e.g. FLIR's Black Hornet and similar micro-UAS are already pairing with ATAK for reconnaissance). Our innovation is in orchestrating a networked swarm for **signal mapping**, a capability that directly addresses SOCOM's need to secure comms infrastructure by *finding and exposing cyber-electronic threats before they can do harm*.

EMW Anchors for Jamming and Decoy Operations

After locating enemy communication nodes or jammers, the second part of our strategy kicks in: **offensive electromagnetic warfare via intelligent anchor nodes**. We term these devices "anchors" because they are typically deployed onto the ground or a vantage point and remain in place to conduct sustained EW operations. **Each anchor is a compact, expendable radio jammer/relay** – roughly palm-sized, battery powered, and equipped with an SDR transceiver. The drones carry a number of these anchors and can drop or position them near target areas (for example, on a rooftop, through a window, or covertly on a perimeter). Once deployed, anchors join the UWB mesh as relays, but **select anchors can be switched into offensive EW mode** under operator command.

1. Targeted Jamming (Denial & Degradation): Anchors can emit **jamming signals on enemy frequencies** to degrade or deny their communications. For instance, if the swarm pinpoints an enemy radio net or jammer, an anchor can be commanded to transmit broad or tailored interference on that frequency band. By using multiple low-power jammers positioned close to enemy emitters, we raise the local noise floor and **disrupt adversary C2 without needing high-power transmitters** (a distributed "swarm jamming" effect). This technique aligns with the Army's finding that raising the noise floor and obfuscating signals can prevent an enemy from pinpointing or understanding friendly emissions – here we apply it offensively against enemy comms. *In effect, the anchors can* ***quiet the enemy's networks*** at critical moments (e.g. just as an assault begins, or to isolate an objective area). Because the anchors are networked and under ATAK control, operators can **remotely dial jamming on/off** or adjust parameters to avoid undue interference to friendly systems. Our system maps friendly vs. enemy spectrum use in real time (via the swarm's sensing) so that jamming is **selective and precise**, focused only on hostile signals. This mitigates the risk of fratricide in the EMS.

Notably, small drones and disposable devices have already been tested as jammers/decoys by the Army. In one exercise, a unit **strapped $30 Raspberry Pi-based jammers to hobby drones to serve as electronic decoys** that confused the enemy with spurious signals. This yielded great effects in forcing the opposing force to waste effort on false targets. Our approach builds on that concept, but with far more integration and automation: the same swarm that detects an emitter can immediately deploy a jammer against it. *For example, upon finding an enemy HQ's radio, the system could drop an anchor that blankets that radio's frequency with noise.* The **distributed nature** of the SWAT Swarm (many small jammers vs. one large jammer truck) makes it *resilient and hard to detect*. If the enemy tries to hunt our jamming source, they might find one tiny anchor – and that too will appear as just another signal/contact on their sensors, possibly alongside decoys, complicating their situational awareness.

2. Decoy Network & Imitative Deception: Perhaps more powerful is the anchor's ability to **mimic communication networks** – creating *"decoy networks"* that the enemy may connect to or be misled by. This capability directly targets the "Protect Infrastructure through Cyber-threat Emulation" aspect of SPICE: we emulate

the adversary's own networks to **trick and surveil them**. Each anchor's SDR can be programmed to impersonate various emitters: for example, an anchor might clone the identity of an enemy radio repeater, a cell tower, or a Wi-Fi access point. By doing so, the anchor **lures enemy users or systems to interact with it**, all the while **recording their transmissions or even injecting false information**. This is a form of **imitative electronic deception**, injecting bogus but believable traffic into enemy comms.

A concrete use-case is **fake cell towers**: A dropped anchor could act as a **rogue GSM/LTE base station** (similar to a Stingray device) to force enemy phones to connect to it. This would *deny* them real cell service (a form of jamming through distraction) while simultaneously allowing us to **intercept phone metadata or calls** (surveillance). Law enforcement and military units have used such **IMSI-catcher** techniques for years to monitor targets; our system would deploy it tactically on-demand. Another example is replicating enemy tactical radio networks: after observing their frequency-hopping pattern or network protocol (which our swarm's AI can help classify), an anchor could transmit *dummy network traffic* that looks authentic. This might confuse enemy operators or automated systems – e.g. generating fake "friendly units" on their Blue Force Tracker equivalent, or fake command orders in their chat – if they attempt to digest our decoy transmissions. In training, U.S. units have successfully used emitters broadcasting **false command post radio traffic alongside inflatable decoy vehicles** to mislead adversaries. Similarly, our anchors can project phantom communications nets or false signals to draw enemy attention.

Decoy Effects and Payoff: By **duplicating the enemy's electromagnetic "fingerprints"**, our decoy networks sow confusion. Adversaries may waste time and resources reacting to ghost units or misleading signals. Critically, if the enemy tries to locate these signals, they reveal themselves in the process – *turning their EW sensors against them*. In one Army trial, a brigade **recorded its own command post's signal signature and rebroadcast it from a false location**, causing the opposing force to target the wrong spot and expose their positions. We leverage the same principle offensively: decoy anchors replicate enemy comms to *control the narrative in the spectrum*. All the while, our system captures valuable **ELINT (electronic intelligence)**: every time an enemy interacts with a decoy network, we log their frequencies, protocols, and potentially content of communications. This intel can be fed back into our AI/ML models to improve signal classification and to build profiles of adversary TTPs (tactics, techniques, procedures).

It is important to note that **spectrum deception and jamming must be used judiciously**. Our strategy emphasizes **remote operator oversight via ATAK**. Through the ATAK interface, EW officers or team members can see all deployed anchors on the map (each anchor appears as a friendly icon with its status). They can **tap on an anchor to select jamming or decoy modes**, adjust power levels, or shut it down quickly if needed. This **human-in-the-loop control** ensures deconfliction – for example, an operator will verify that no friendly comms are on a frequency before jamming it. Our system could also integrate with higher-level spectrum management tools (for instance, the Army's emerging Spectrum Situational Awareness System) to further automate deconfliction. Ultimately, the combination of **triangulation by drones and immediate electronic attack by anchors** gives SOF a unique capability: *find the threat and finish the threat in the EM spectrum*, in real time.

Command and Control Integration (ATAK & Blue Force Tracker)

Seamless C2 integration is a cornerstone of our approach, ensuring that the SWAT Swarm's capabilities plug directly into existing team workflows. ATAK is the primary user interface: operators receive swarm updates and issue commands through the familiar ATAK maps and plugins. This is feasible because ATAK already supports custom network feeds and is used widely for sensor integration; in fact, ATAK has been likened to a modern **Blue Force Tracker app**, showing where friendly assets are and ingesting tactical data. Our system treats drones and anchors as *team assets* within ATAK. Each drone's telemetrics and each detected emitter can appear as icons on the map. For example, as drones move, their icons update; when a drone flags an enemy signal, an icon (perhaps a red diamond) is dropped at the estimated location of that signal. The user can click that icon to see details (frequency, type, time detected). This provides instant **situational awareness of the EM environment** to the team on the ground, who can then decide on actions (e.g. investigate that room, or cue a direct strike).

Integration with **Blue Force Tracking (BFT) systems** and the wider force network is achieved via **standard message formats**. Our use of Cursor-on-Target for ATAK means that data can be gatewayed to other networks. The Army's latest Mission Command software (e.g. **JBC-P / MMC-S**) is being built to translate ATAK's CoT messages into the Variable Message Format (VMF) used by legacy BFT systems. This ensures that the **common operational picture** at higher echelons will also include our swarm's intel. In practical terms, when our system geolocates an enemy jammer, that location can be transmitted up to a headquarters and marked on the COP for all friendly units – enabling, say, an aircraft or artillery unit to be tasked to neutralize it. By design, our architecture is **interoperable with NATO standards** as well; for instance, the Blue Force Tracker concept is based on sharing GPS-derived

positions of friendly (blue) and enemy (red) forces. Here, our drones essentially generate *pseudo-GPS coordinates* for otherwise invisible enemy electronic assets, and push those to the network. This interoperability and **data sharing are crucial for Phase III transition**, as the technology must plug into larger DoD infrastructure.

C2 Use Case: Consider a Special Forces team moving to raid a high-value target in a denied area. Team members have ATAK on ruggedized phones. They launch the SWAT Swarm ahead of the assault. As the swarm navigates a compound, ATAK live-updates with icons for several detected devices: perhaps a Wi-Fi signal upstairs (possibly an enemy router) and a VHF push-to-talk radio in a back room. The commander on ATAK sees these and can make decisions – e.g., isolate that back room first because it's an enemy radio operator. At the same time, one drone loses link because of a subterranean area; ATAK shows its signal lost – so the team deploys an **anchor node to restore comms** (ATAK might even recommend this). During the raid, intel analysts in the tactical operations center, via the BFT network, see in real time that jammers deployed by the swarm are active on enemy comm channels (this might show as an icon or message "Jamming ON"). They also see an enemy QRF (quick reaction force) trying to call for help on a net that we are spoofing – allowing US forces to anticipate and intercept. All of this is enabled by the tight integration of our system with existing **digital C2 ecosystems**.

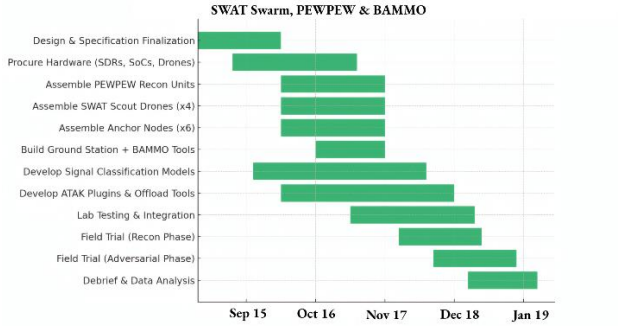
Phase I Work Plan and Feasibility

In Phase I, we will **prove out the key components** and demonstrate a basic integrated system in a controlled environment. Our plan includes:

- **Component Feasibility Testing:** We will prototype a micro-UAV node and an anchor node. For the UAV, we will adapt a small quadcopter (similar to the Crazyflie or other COTS mini-drone) to carry an SDR (e.g. a low-cost RTL-SDR or Ettus B200-mini) and a lightweight compute board (e.g. Raspberry Pi Zero 2 or ARM Cortex M7 with TensorFlow Lite). On the anchor side, we will build a battery-powered UWB radio module (Decawave-based) paired with an SDR chip capable of transmit/receive in targeted bands. These prototypes will validate **size, weight, and power (SWaP)** constraints – ensuring the drone can lift the payload and the anchor battery can support at least ~30 minutes of operation. We anticipate using palm-sized anchors weighing under 100 grams (as described in our design). If needed, multiple anchor types (pure relay vs. jammer-capable) will be considered for optimal SWaP. *Outcome:* Verify that hardware components meet flight and comms requirements.
- **Mesh Network & Localization Demo:** Set up a simple UWB mesh with at least two anchors and one UAV. In a large room or outdoor area, test multi-hop communication and ranging. We will measure the achievable range of UWB links (which should be tens of meters indoors) and the accuracy of ranging between nodes. We will also simulate an **RF emitter** (e.g. a Wi-Fi router or walkie-talkie) in the environment and have the UAV/anchors collaborate to locate it. Even with just one drone and two anchors (forming a triangle), we can demonstrate localization by moving the drone around the emitter and computing position via trilateration. *Outcome:* Show that the system can relay data through anchors and calculate emitter positions to within a few meters or better.
- **AI Signal Classification:** Develop or port a small **ML model** that runs on the drone's processor to classify signal types. Using labeled RF signal datasets (or synthetically generated waveforms), we will train a model (e.g. a CNN on spectrogram input) to recognize a handful of signal classes – for Phase I likely Wi-Fi and analog radio as a proof of concept. We'll then deploy this model on the drone and test in real time: the drone's SDR will sniff signals and the onboard AI will output what type of signal it is detecting. *Outcome:* Demonstrate that a drone can autonomously identify, for example, a Wi-Fi hotspot vs. a FM radio signal with reasonable accuracy, within the constraints of limited processing. This validates the "smart sensing" aspect.
- **End-to-End Emulation Scenario:** Integrate the pieces for a mini **SPICE scenario laboratory demo**. We will set up a mock "enemy network" using a Wi-Fi router (for a data network) and a two-way radio (for a voice net) as targets. The UAV (with anchors pre-loaded) will be released in this environment (e.g. a building or maze) with no GPS. It will navigate a short route, detect the signals, drop an anchor to maintain comms when needed, and send back detections to an **ATAK workstation**. We will use an ATAK plugin or script on a laptop to ingest the CoT messages from the drone via a local gateway, displaying icons for the detected "enemy router" and "enemy radio." We will also activate the **EW function** in this demo in a limited, safe manner: for instance, commanding the anchor to imitate the Wi-Fi network (creating a fake SSID) or jam the router's channel. This will allow us to observe the effect (e.g. verify the target device's connectivity is disrupted or that it connects to the decoy). *Outcome:* A live demonstration that combines **exploration, detection, reporting, and EM attack** – achieving a TRL-4/5 level proof-of-concept in a relevant environment.

Throughout Phase I, we will identify and address key risks. **Weight/Payload** is a known challenge – if the SDR and battery prove too heavy, we have backup plans such as using multiple slightly larger drones or tethered power for

test purposes. **Mesh interference** is another consideration: we will test that our jamming signals do not unduly degrade the UWB mesh (by design, UWB operates in different spectrum and is resistant to narrowband interference). We will also ensure **safety and deconfliction** in the lab (using shielding or anechoic enclosures for any jamming tests to comply with FCC regulations). By the end of Phase I, we aim to deliver a technical report and demonstration that convinces evaluators of the approach's merit and feasibility.



Commercialization and Transition Strategy

This dual-use technology has strong transition potential within DoD and beyond. **Primary customer** alignment is with USSOCOM's **PEO SOF Warrior** communications and electronic warfare programs – the system could transition into a Program of Record providing SOF teams with organic spectrum reconnaissance and attack capability. We will work closely with SOCOM end-users through experimentation events (e.g. SOFWERX tech showcases) to refine operational concepts. The capability also has broad appeal to the conventional military: the U.S. Army is actively investing in **electromagnetic decoy and obfuscation tools**, as seen in recent brigade experiments with drone-borne decoys and systems like *MAGPIE* that fake command post signals. Our solution could augment Army brigades or Marine units by offering a **lightweight, rapidly deployable EW toolkit** – especially as the Joint force shifts towards *distributed operations and needs low-cost decoys*. We anticipate engaging Army program offices (PEO IEW&S, etc.) for Phase III opportunities, leveraging the SBIR results and SOCOM buy-in as validation.

Beyond the military, there are **law enforcement and homeland security applications**. The system's ability to locate and jam rogue communications is relevant to FBI HRT or police SWAT teams (e.g. to find a kidnapper's phone in a building, or to cut off terrorist communications during an intervention). Agencies like DHS could use the drone swarm to **secure critical infrastructure** by detecting illegal surveillance devices or jammers. In the private sector, the **telecom industry** might use portions of this tech for network testing – e.g. drones that map cellular coverage or detect interference sources on their towers. There is also a niche market in **search and rescue**: a similar swarm could find signals from missing persons' cell phones or emergency beacons in disaster areas, a clear lifesaving application. We plan to pursue these dual-use avenues by partnering with established vendors: for example, teaming with a tactical radio manufacturer or a drone company to co-develop a product. The core components (mesh networking, RF classification AI, and decoy techniques) could be spun off as modules in larger systems – such as integrating our signal-mapping AI into a next-gen Blue Force Tracker software, or offering the decoy emitter as a standalone **training range tool** for the military (to emulate adversary signals during exercises).

Conclusion

In summary, our strategy for the SOCOM SPICE SBIR is to integrate **autonomous drone-based signal scouting** with **offensive electromagnetic warfare anchors**, all under the umbrella of existing tactical C2 systems. This approach provides a **full-spectrum solution**: find the communication threats, fix their location, and finish their effectiveness through jamming or deception – in essence, *"Detect, Deceive, Disrupt."* By leveraging modern micro-UAV swarming, AI/ML for signal analysis, and proven EW tactics in a novel combination, we address both the **technical feasibility** and the **operational relevance** required by this SBIR. Our concept directly tackles the challenges of contested communications that SOF operators face, turning those challenges into an opportunity: the chaos of the electromagnetic domain becomes a playing field we can dominate. The research and results from Phase I will solidify the concept, while setting the stage for Phase II prototyping of a robust system. With strong transition pathways to SOCOM and other military users – and exciting dual-use possibilities – this project exemplifies the innovation envisioned by the SBIR program. It will **secure and protect friendly infrastructure** by actively **emulating and overwhelming cyber/EW threats**, keeping our forces one step ahead in the electromagnetic battle space.