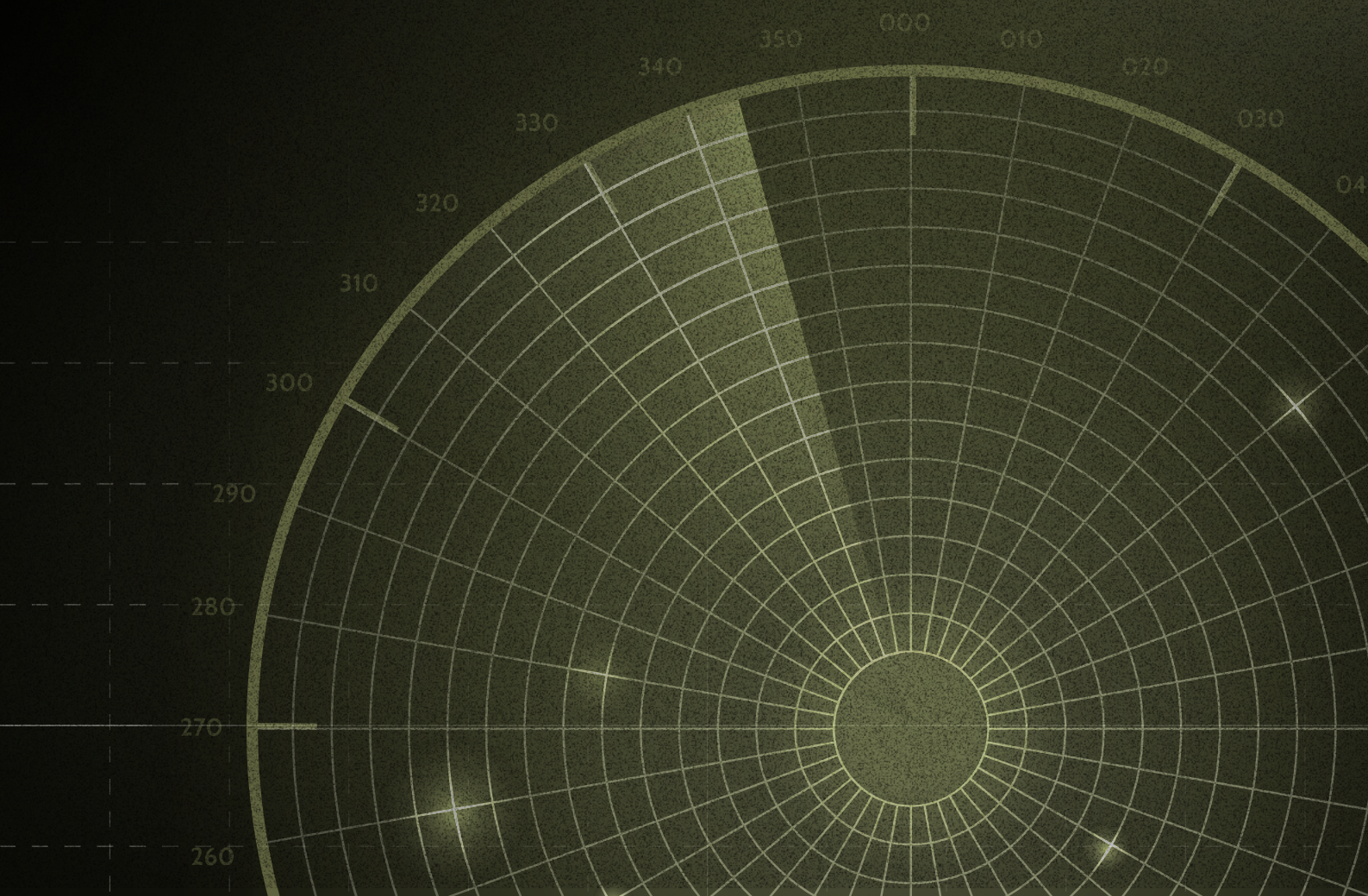
SNAKE ISLAND INSTITUTE

AB3 Tech

Detect, Jam, Locate: A Hacker's Guide to Battlefield Signals

AB3 TECH and Snake Island Institute

European Defense Tech Hackathon,
Lviv, May 22-25 2025



Introduction

Thank you for participating in the first-ever Defense Tech Hackathon built inside an active fighting brigade.

The 3rd Assault Brigade is one of Ukraine's most effective fighting units, and for the first time, they've opened up their real frontline challenges to the world's top innovators, inviting each and every one of you to solve real problems, with a potential to save real lives. These are not hypothetical prompts. Each one is based on real constraints, needs, and failures observed on the ground.

This booklet is an overview of a selection of problems from the drone challenge section of the hackathon, made by the Snake Island Institute in partnership with AB3 Tech. These challenges range from technical issues with drone signal jamming and early warning systems, to more complex questions around operator geolocation and signal analysis. In most cases, the descriptions here are only a starting point. The details of each problem — and what a useful solution might look like — will become clearer through discussion with soldiers and subject-matter experts during the hackathon.

Where possible, we've included background information, current methods, key limitations, and relevant sources. This is not an exhaustive technical document, and it's not meant to prescribe exact solutions. It's meant to give you just enough structure to begin testing, building, and iterating.

Good luck.

Viktoriia Honcharuk,
Hackathon Organizer, Head of Projects, Snake Island Institute

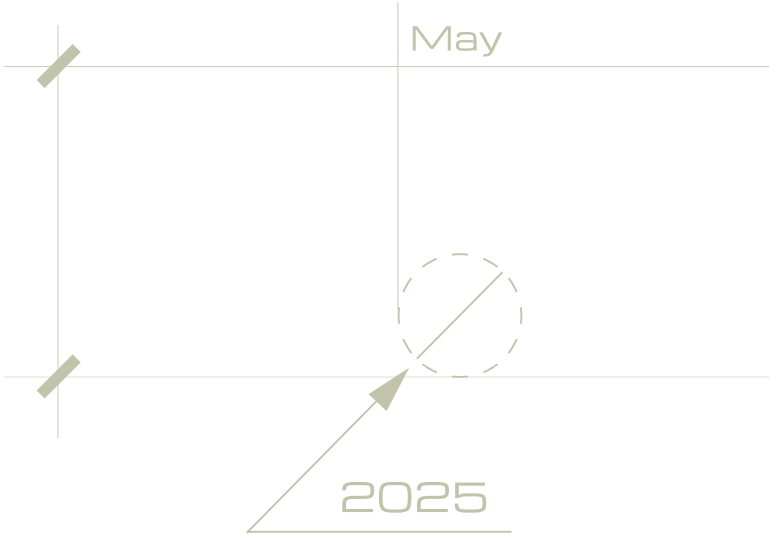
Catarina Buchatskiy,
Director of Analytics, Snake Island Institute

About the Snake Island Institute

The Snake Island Institute (SII) is an organization dedicated to fortifying the strategic partnership between Ukraine and the United States, with a focus on defense analytics, institutional cooperation, and sustained security support. Snake Island's work includes:

- **Analytics:** Advancing understanding of modern warfare and doctrine.
- **International partnerships:** Aligning Ukrainian, U.S., and international decision-makers.
- **Defense Tech:** Enabling battlefield integration of critical technologies.
- **Strategic Development:** Building future-ready security frameworks.

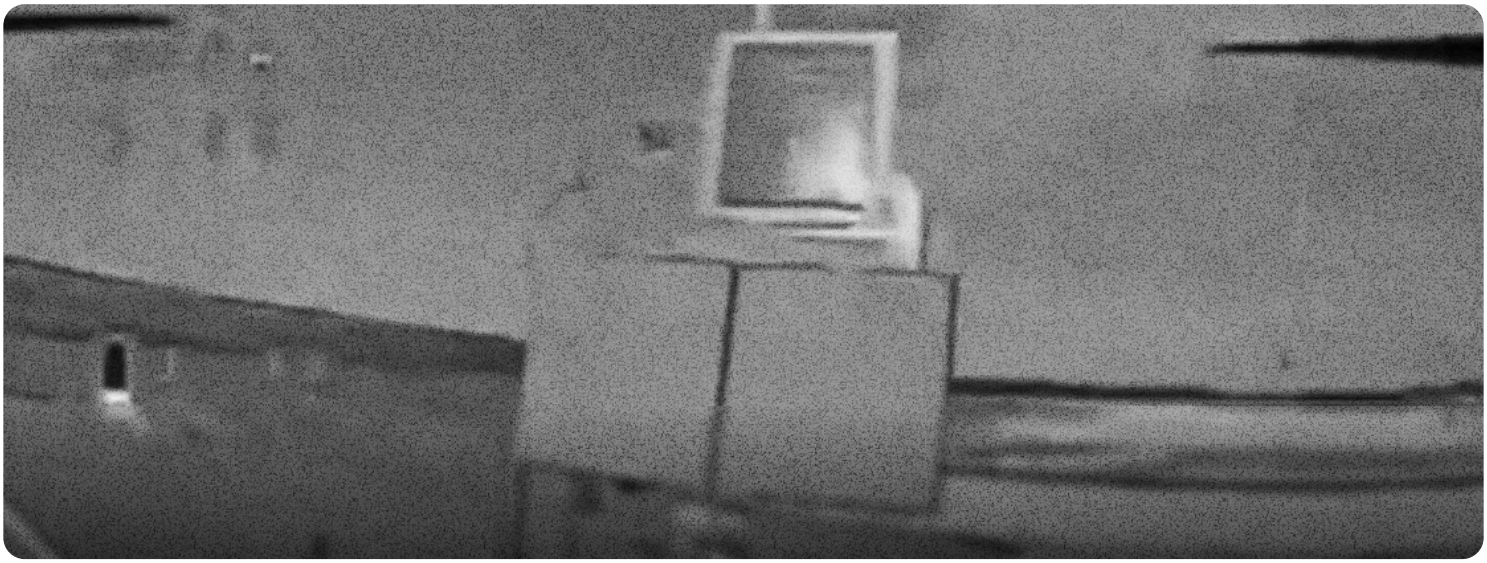
We work closely with both U.S. and Ukrainian defense stakeholders to strengthen frontline effectiveness, inform strategic policy, and ensure long-term defense readiness.



DYNAMIC FREQUENCY FPV DRONE JAMMING

Since the proliferation of FPV drones on the frontlines, the cat-and-mouse game between drones and drone jammers has become a defining feature of modern war. The modular construction of FPV drones means they're able to adapt quickly to emerging electronic warfare techniques, and drone jamming has become significantly more sophisticated in response.

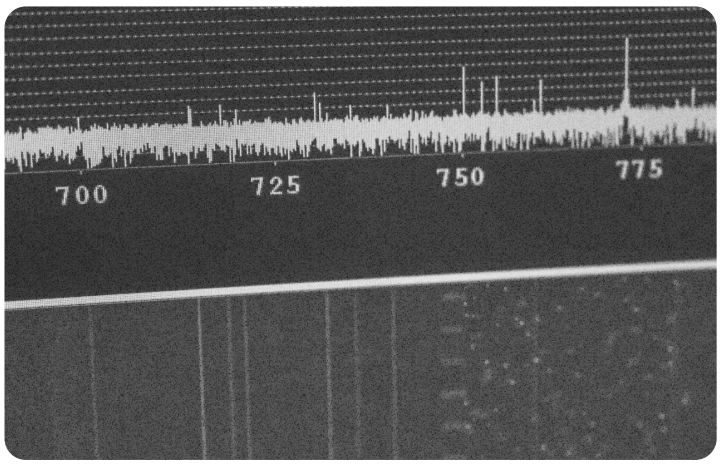
Jamming drones involves targeted interference with the radio signals that drones use for communication with the operators, by transmitting signals on the same frequency as the control link to overwhelm its communications, rendering the drone non-functional — jammed.



A Chernyi Glaz system fielded in the Ukrainian warzone / Image credits: Serhii Flash, Ukrainian Armed Forces

Techniques used for RF jamming include:

- **Broadband Jamming:** Transmitting high power noise across a broad range of frequencies, covering the drone's communication channels.
- **Spot Jamming:** Focusing on a specific frequency band used by the drone, providing a more targeted and efficient disruption.
- **Barrage Jamming:** A combination of broadband and spot jamming, targeting multiple frequencies simultaneously to ensure disruption.



A visualization of the rapidly-changing frequencies of the Himera military radio, which features signal-hopping technology that makes it difficult to jam. Credit...Brendan Hoffman for The New York Times

In response to targeted frequency jamming, engineers started incorporating frequency-hopping into drone systems, which allows a drone to jump quickly between frequencies to bypass the ones that are blocked...the adversary has also incorporated this technique, which means that naturally, in response, it's time for dynamic frequency jamming systems.

These systems should be designed to adaptively scan and identify the communication frequencies being used by drones and jam the signals accordingly.

TECHNICAL CHALLENGES IN DYNAMIC FREQUENCY JAMMING

The transition from static to dynamic jamming systems presents several technical challenges that need to be addressed to ensure effective drone disruption:

A Chernyi Glaz system fielded in the Ukrainian warzone / Image credits: Serhii Flash, Ukrainian Armed Forces

01

ADAPTIVE SCANNING TECHNIQUES:

Developing adaptive scanning techniques is crucial for dynamic systems. These techniques involve continuously monitoring a range of frequencies to detect and target those used by drones. The effectiveness of adaptive scanning relies on the ability to quickly identify and switch frequencies to match the drone's communication patterns.

02

FREQUENCY HOPPING COUNTERMEASURES:

Enemy drone operators often employ frequency hopping to evade jamming. This involves rapidly switching between different frequencies, making it difficult for static jamming techniques to disrupt their communication. Dynamic systems must be capable of not only detecting these frequency changes but also adapting in real-time to maintain jamming effectiveness.

Source: (MDPI, Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study), (Euromaidan Press, 2025), (Euromaidan Press, 2024)

HELPFUL HINTS...

SIGNAL PROCESSING ALGORITHMS:

Advanced signal processing algorithms are **essential** for analyzing and identifying frequency patterns used by drones. These algorithms enable dynamic systems to adapt quickly to changing frequency environments.

SOFTWARE-DEFINED RADIOS (SDR):

SDRs are interesting for dynamic jamming because they offer the flexibility to scan and transmit across a broad range of frequencies without changing hardware. Wideband SDRs can monitor larger portions of the spectrum at once, increasing the chances of detecting the drone's control signal in real-time.

MACHINE LEARNING MODELS:

Machine learning models, particularly reinforcement learning and anomaly detection models, can be trained to recognize patterns in the RF environment. These models help in predicting frequency hopping behavior, identifying control signals buried in noise, and selecting the optimal frequencies to jam. Over time, they can adapt to evolving tactics and even generalize across different drone types.

REAL-TIME SIGNAL DETECTION AND RESPONSE

Require fast processing of large amounts of RF data. **FPGAs (Field-Programmable Gate Arrays) and GPUs (Graphics Processing Units)** can accelerate the signal analysis and classification tasks that SDRs alone can't handle efficiently. FPGAs are especially useful in low-latency environments and can be tailored for specific filtering or detection operations. GPUs excel at running complex algorithms — such as neural networks or clustering models — in parallel, which is useful for spectrum analysis and anomaly detection.

DIRECTIONAL ANTENNAS

focus the jamming signal in a specific direction, increasing effectiveness while reducing collateral disruption to friendly systems. They also allow for more precise triangulation of drone and operator positions, which is useful when combined with geolocation tools. While omnidirectional antennas are simpler, they waste power and can risk detection.

ACCURATE DETECTION AND ANALYSIS OF FPV CONTROLLER SIGNALS

OVERVIEW OF FPV CONTROLLER SIGNALS

FPV technology is central to modern drone piloting. It enables real-time control and feedback by transmitting a live video feed and command signals between the drone and the operator — typically over the 5.8 GHz band for video transmission, while control signals often use 2.4 GHz, 915 MHz, or other bands depending on the protocol.

Each FPV drone is tethered to its pilot by this wireless uplink. If you can detect that link, you can potentially jam it. If you can analyze it, you may even be able to locate the operator.

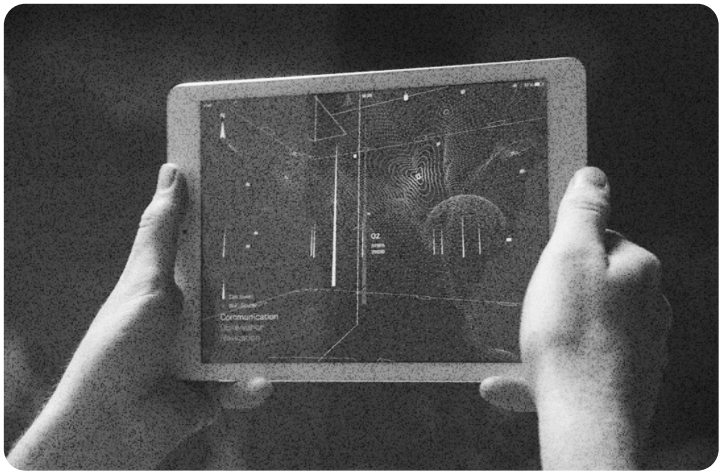
In most current defense systems, detection focuses on drones in flight — using visual, acoustic, or RF signatures to identify threats once they're airborne. But by that point, the drone is already approaching its target. A more effective approach is detecting the controller's uplink before the drone ever takes off.

In the early stages of the war, RF signal detection was mostly trial and error. EW teams relied on basic spectrum analyzers and consumer SDRs to scan likely frequency bands and look for signs of activity — a signal spike here, some video feed noise there. This manual process was slow, imprecise, and struggled in crowded RF environments filled with Wi-Fi, Bluetooth, and other background chatter.

As FPV drones became more widely used — and as electronic warfare teams became more experienced — it became clear that this problem needed faster, smarter solutions. Detection work that used to be manual and reactive is now trending toward automated classification, real-time alerting, and even machine learning-based prediction.

The goal now is to identify control signals in real time, even in noisy environments, and extract enough information to assess their intent — whether they're idle, arming, or actively guiding a drone in flight.

The challenge is to build a signal intelligence module that can operate passively — no transmissions, no jamming — and still deliver actionable information.



SDK

A strong system should be able to:

- Detect and classify FPV controller signals across multiple popular protocols (e.g., DJI, ELRS, Crossfire, Ghost)
- Estimate signal strength and proximity, even in noisy RF environments
- Recognize behavioral patterns — is the operator idle, arming, or actively flying?
- Trigger alerts or record spectral snapshots for further analysis or targeting

This level of signal intelligence can make a real difference at the tactical edge, especially for teams trying to anticipate drone launches before they happen.

HELPFUL HINTS...

01

Use wideband SDRs to continuously monitor control frequency bands (typically 868/915 MHz, 2.4 GHz, and 5.8 GHz). The goal is to passively observe traffic patterns and extract identifying features.

02

Even among drones using the same protocol, minor hardware differences create subtle variations in signal characteristics. RF fingerprinting methods can help you distinguish between devices, identify reused controllers, or track operator movement.

03

ML models can help classify states (idle, arming, active flight) based on timing, power, and modulation characteristics. You might train a lightweight classifier using labeled examples to detect transitions between states.

04

Directional antennas can help estimate location or bearing. Rotating arrays can support basic triangulation.

05

RF congestion is real. You'll need filtering and intelligent thresholding to avoid false positives.

RELIABLE EARLY DETECTION AND WARNING OF APPROACHING DRONES

OVERVIEW OF EARLY DETECTION SYSTEMS FOR UAVS

As drone threats become faster, smaller, and harder to see, frontline units are often left with only a few seconds to react. Today's detection systems are still playing catch-up. Most were built for larger aircraft — not for fast, low-flying FPV drones that can appear and strike within seconds. The challenge now is clear: we need reliable early warning systems that can spot these threats before they're already overhead.

The best chance at early detection doesn't lie in any one sensor. It lies in combining several.

Early drone detection systems were extensions of traditional air defense — radar towers and visual spotters retooled for smaller targets. But those systems weren't designed for FPVs flying at treetop level or diving through windows.

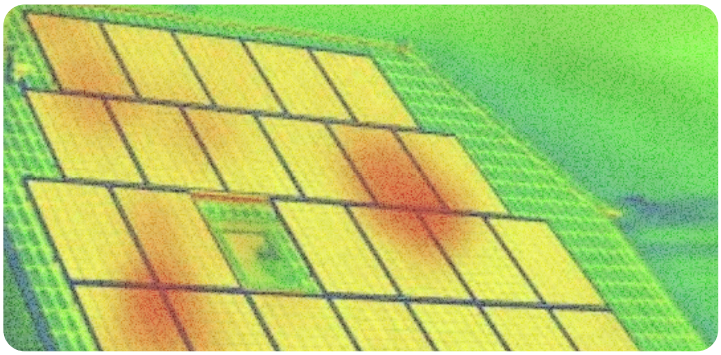
Radar, the backbone of most aerial surveillance, struggles to pick up small UAVs with low radar cross-sections. Even upgraded micro-radar units can be confused by birds, ground clutter, or terrain masking.

Acoustic detection — listening for the sound of drone motors — was introduced as a low-cost alternative. But it has its limits too: background noise, wind, and the increasingly quiet motors on newer FPVs all make reliable audio detection harder.

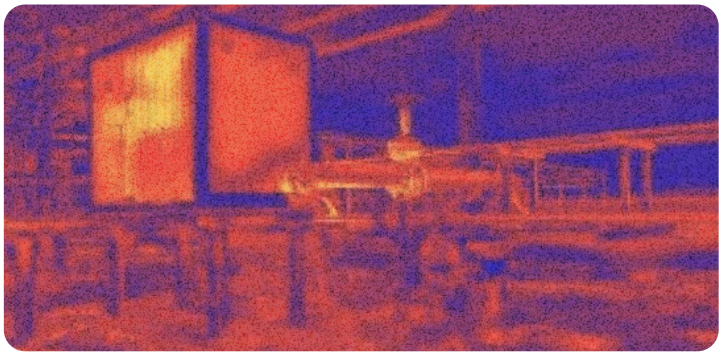
Optical and infrared sensors have the advantage of visual confirmation, but they're highly dependent on lighting, weather, and line of sight. In fog, at night, or behind trees, they may fail completely.

What makes sense now, and what many teams are starting to prototype, is **multi-sensor fusion**.

By layering data from radar, audio, and optical sensors, and using AI to interpret it, we can build systems that are more reliable, more accurate, and more resilient to environmental noise. Where one sensor drops out, another can still track. Where noise or birds might confuse a radar ping, machine learning models can learn to tell the difference.



Solar Hotspot. Image Credit: Avantier Inc.



Building Inspections. Image Credit: Avantier Inc.

TECHNICAL CHALLENGES IN DETECTING SMALL UAVS

Detecting small UAVs presents several technical obstacles:

DATA FUSION REQUIREMENTS:

Single sensor systems often prove inadequate. Combining data from multiple sensor types—known as multi-sensor fusion—can significantly enhance detection reliability.

ENVIRONMENTAL CONDITIONS:

Factors such as weather, terrain, and urban environments can significantly impact sensor performance.

LOW SIGNAL PROFILE:

UAVs are designed to be unobtrusive, often resulting in a low signal profile that complicates detection efforts.

Sources: ResearchGate, 2025

The goal is to build a multi-sensor detection module that works in real-world battlefield conditions. That means:

- Fusing radar, acoustic, and optical inputs
- Using beamforming microphones to localize drone audio, even in noisy settings
- Deploying micro-radar systems that track movement patterns rather than just raw reflections
- Integrating thermal or IR cameras to detect heat signatures in low-light conditions
- Applying AI to classify objects, track trajectories, and filter out noise or irrelevant motion

And importantly:
this system needs to operate with low latency, possibly even triggering automated countermeasures like jammers or alerts to nearby units.

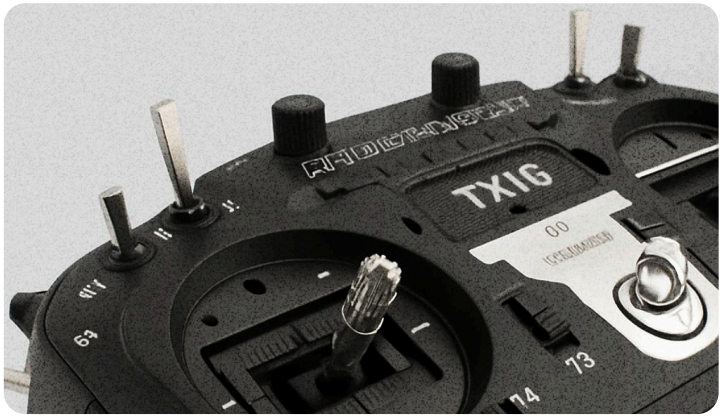
SENSOR TYPE	CHALLENGES	INNOVATIONS
RADAR	Low radar cross-section of UAVs	High-resolution radar
ACOUSTIC	Environmental noise interference	Sophisticated noise differentiation algorithms
OPTICAL	Visibility limitations	Enhanced imaging technologies

GEOLOCATION OF DRONE OPERATORS USING SIGNAL ANALYSIS

As drones become faster, smaller, and easier to replace, the operator becomes the more valuable — and vulnerable — target. Disrupting or neutralizing an FPV drone in flight can buy time. But finding and stopping the operator can eliminate the threat entirely. This makes geolocation of the uplink (the signal sent from the controller to the drone) a critical objective.

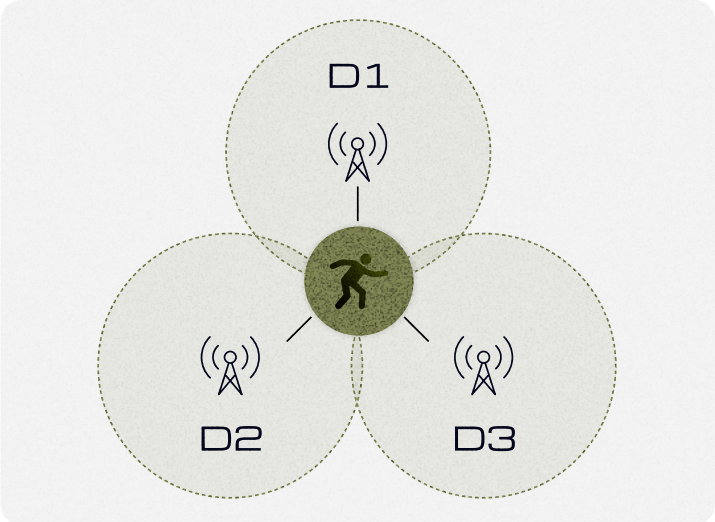
The uplink signal from an FPV controller is usually low-power, highly directional, and short in duration. In rural or open terrain, you might get a clean line-of-sight reading. In dense or urban environments, however, that signal reflects off buildings, terrain, and other obstacles — creating multipath distortion that makes precise geolocation extremely difficult.

Operators also don't make things easy. Many now use techniques to deliberately obfuscate or disguise their signal: altering modulation, hopping frequencies, or encrypting transmission patterns. In short, they know we're listening — and they're trying not to be found.



TX16S MKII Radio Controller

OVERVIEW OF FPV CONTROLLER SIGNALS



TRIANGULATION:

One of the simplest approaches. Take directional signal measurements from at least two known locations and compute where they intersect. This works in theory, but in practice, the accuracy depends heavily on how precisely you can measure the incoming angle and how much noise, reflection, or signal loss is present.

TIME DIFFERENCE OF ARRIVAL (TDOA):

TDOA works by calculating how long it takes a signal to arrive at multiple receivers. From the timing differences, you can derive a hyperbolic position estimate. It's powerful, especially for fast-moving operators or drones, but it requires tight clock synchronization between all receivers, down to nanoseconds. GPS-disciplined oscillators or other high-precision timing hardware is essential.

ANGLE OF ARRIVAL (AOA):

AOA systems use antenna arrays to measure the angle at which a signal hits the sensor. With multiple AOA sensors, you can estimate a position similarly to triangulation, but with better resolution. These systems are effective but often bulky or fragile, and their accuracy degrades quickly in cluttered RF environments.

SIGNAL FINGERPRINTING:

Beyond location, there's identity. Every transmitter has small, unique imperfections, whether in frequency drift, phase noise, power signature... Signal fingerprinting captures these traits and can be used to match signals to known emitters, even if the operator is mobile. This is especially useful for tracking repeat users, identifying reused gear, or recognizing spoofing attempts.

A strong system should be able to:

- Detect and classify FPV controller signals across multiple popular protocols (e.g., DJI, ELRS, Crossfire, Ghost)
- Estimate signal strength and proximity, even in noisy RF environments
- Recognize behavioral patterns — is the operator idle, arming, or actively flying?
- Trigger alerts or record spectral snapshots for further analysis or targeting

HELPFUL HINTS...

To locate operators reliably, you'll likely need to design a multi-receiver system using synchronized SDRs.

These receivers should be:

01 **Distributed** over several hundred meters or more.

02 **Time-synced** via GPS or shared clock for TDOA accuracy.

03 **Directional** where possible, to support AOA triangulation.

04 **Connected** to a central processor for real-time fusion and mapping.

On the software side, you'll need:

01 **Signal detection & classification algorithms.**

02 **Geolocation computation modules** (TDOA/AOA hybridization is ideal).

03 **Visualization tools** to map emitter positions and track movement.

04 **Optional: RF fingerprinting models** to flag known emitters or suspicious behavior.

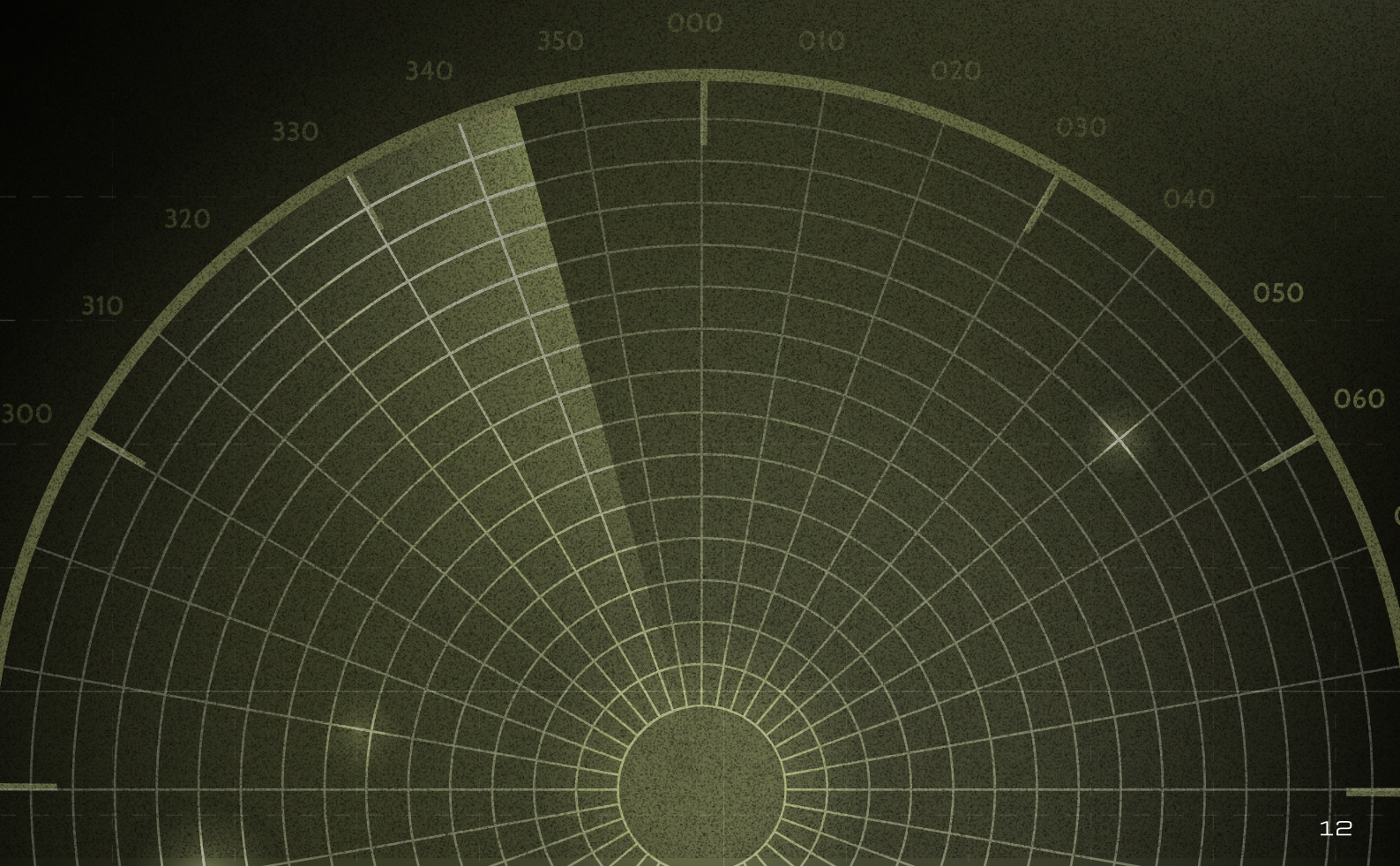
Conclusion

The systems you build here won't be evaluated by pitch decks or polished demos. The only real measure of success in modern defense technologies is battlefield testing in Ukraine.

At the Snake Island Institute, we partner with AB3 Tech to ensure that promising solutions can be tested at the front quickly. With real users, under real constraints. At battlefield tests, you'll encounter constraints that don't show up in a lab. Broken data links, signal interference, field conditions that make even basic assumptions unreliable. That's part of the process. The best systems don't just perform well in theory, but survive contact with the real world.

The Snake Island Institute is helping bridge the gap between innovation and implementation. As we said in the introduction, we're focused on enabling battlefield integration of critical technologies, advancing modern warfare analytics, and strengthening the long-term defense architecture between Ukraine and its allies.

Thanks for building with us today.



AB3 Tech

SNAKE ISLAND INSTITUTE