Jamming Drone — Risk Assessment (Mini Case Study)

AI Governance · Compliance · Technical Risk · Safety & Operational Risk

Prepared by: Mohamed Elkasabi, GRCP, GRCA

Date: October 2025

Portfolio Work — IT Risk & Advisory Track

Jamming Drone — Risk Assessment (Mini Case Study)

1. Executive Summary

This assessment applies a formal risk-management approach to an academic prototype exploring AI-based camera detection and simulated signal disruption on a drone platform. The project introduces exposures across four domains: legal/compliance, physical safety, ethical/reputational, and technical reliability. Each risk was scored, analyzed, and mapped to controls.

Key mitigations include use of software emulation instead of live jamming, controlled testing environments, pre-flight safety procedures, and restricted code disclosure. After mitigation, residual risks fall within acceptable tolerance for academic research, demonstrating that high-risk concepts can be executed responsibly under structured controls.

2. Context & Scope

This assessment covers risks arising from the design and testing of a drone-based prototype that integrates AI-based camera detection with a simulated signal-disruption module. The objective is to determine whether the project can be executed within acceptable legal, ethical, safety, and technical boundaries in an academic research environment.

Scope includes

- Hardware integration (Tello drone, ESP32, payload)
- AI-based camera detection logic and dataset usage
- Simulation of jamming behavior in controlled conditions
- Indoor/lab-based testing and restricted documentation release

Out of scope:

- Live RF jamming in public or uncontrolled settings
- Field deployment for law enforcement or tactical operations
- Commercialization or non-academic use

3. Assumptions, Constraints & Boundaries

Assumptions

- All testing is conducted under supervisor-approved and controlled conditions.
- Signal disruption is implemented only through emulation or shielded environments.
- AI evaluation is performed using predefined or controlled datasets.

Constraints

- Compliance with institutional safety and legal policies is mandatory.
- Hardware limits of Tello/ESP32 (battery, payload, processing) constrain testing and reliability.
- Time and resources restrict validation to proof-of-concept, not production assurance.

Boundaries

- No assessment of real-world tactical deployment.
- No optimization of live jamming capability.
- No collection of personally identifiable data beyond academic allowances.

These conditions define the lens through which risk conclusions must be interpreted.

4. Risk Categories Considered

To ensure full coverage, risks were grouped into the following domains:

- **Legal & Regulatory Risks**: compliance with RF, privacy, and research policies
- **Safety & Operational Risks**: flight, lab safety, physical environment
- **Ethical & Reputational Risks**: misuse, misinterpretation, publication exposure
- **Technical & Reliability Risks**: model errors, integration failures, instability
- **Project & Execution Risks**: approvals, resource gaps, timeline constraints

5. Risk Register Snapshot

The complete risk register, including likelihood, impact, scoring, control ownership, and status, is provided separately in **Risk_Register.xlsx**.

It covers legal, safety, technical, ethical, and operational risks, with both current and recommended controls.

Maintaining the register separately supports traceability, version control, and audit readiness.

6. Mitigation Strategy Narrative

Risks are managed through design constraints, procedural controls, and restricted execution. Legal and compliance risk is contained through use of emulation and supervisor oversight. Safety risks are reduced through controlled indoor testing, staged integration, PPE, and formal checklists. Technical risks are addressed via incremental validation, watchdog failsafes, and dataset verification with human review.

Operational risks (approvals, knowledge gaps, equipment limits) are contained through early engagement with institutional stakeholders, literature-based substitution where full testing is not permitted, and structured planning around hardware limits. Ethical and misuse risks are mitigated through disclaimers, redaction of sensitive implementation details, and controlled sharing. With controls in place, residual risk is acceptable for an academic prototype.

7. Residual Risk & Acceptance Statement

Post-mitigation, all high-impact risks are reduced to low or moderate levels. The remaining residual risks are acceptable given the academic context, controlled testing, and supervision. No uncontrolled RF activity or unsupervised flight will take place.

8. Evidence & Controls Retention

Supporting evidence, including supervisor approvals, safety checklists, test logs, and simulation outputs, will be archived and referenced in **Risk_Register.xlsx** for auditability, defensibility, and future review.

9. Limitations & Dependencies

Limitations

- No live RF jamming impact is assessed.
- AI performance is validated on controlled rather than real-world environments.
- Tactical or law-enforcement effectiveness is not within scope.
- Residual risk tolerance is calibrated to academic, not industrial, standards.

Dependencies

- Institutional approvals must remain valid.
- All work must continue under the defined constraints.
- Mitigations (emulation, restricted release, safety controls) must remain active.
- Any scope change requires reassessment.

10. Conclusion

This assessment confirms that the Jamming Drone prototype can be executed responsibly within controlled academic boundaries. The risks are identified, scored, mitigated, and monitored, demonstrating applied competence in structured IT risk assessment and research governance.