Research Plan: “Cyconetic Air-Globe for Honeybee Neurorights & Governed AI Security”

- The Cyconetic Air-Globe system will be enhanced to protect honeybees in high-pollution, high-EMF urban environments.
- A Rust-based governance architecture will be upgraded to enforce secure, role-based access control and prompt-injection resistance.
- Real-time environmental monitoring, neurorights-based EMF mitigation, and governance-grade data integrity will be integrated.
- The system will ensure biological efficacy for honeybees and digital security for human stakeholders.
- A multi-phase research plan will be executed over 6–8 months with a budget of approximately $55,000.

Introduction

Honeybees are vital pollinators facing unprecedented threats from urban environmental pollution and electromagnetic field (EMF) exposure. Concurrently, the digital governance of AI systems managing environmental data and control actions must be robust against adversarial attacks and misuse. This research plan proposes a comprehensive, multi-phase approach to enhance the Cyconetic Air-Globe system for honeybee protection in high-pollution, high-EMF urban environments while simultaneously upgrading the Rust-based governance architecture of the Cybo-Air repository. The goal is to ensure secure, role-based access control, prompt-injection resistance, and augmented rights for verified stakeholders—all integrated into a unified system that is both biologically effective and digitally secure.

Phase 1: Biological & Environmental Protection System (6–8 weeks)

Objectives

- Develop a real-time adaptive protection system for honeybees in urban pollution/EMF zones using the Cyconetic Air-Globe framework.
- Expand the Cybo-Air CEIM/NanoKarma framework to include honeybee-specific hazard weights for chemical and EMF threats.
- Integrate real-time environmental monitoring with biological feedback loops to dynamically adjust protection measures.

Key Tasks

Pollutant & EMF Threat Modeling

- **Task**: Expand the existing Cybo-Air CEIM/NanoKarma framework to include honeybee-specific hazard weights for chemical threats ($PM_{2.5}$, NO_x, O_3, VOCs, heavy metals, neonicotinoids) and EMF threats (5G, Wi-Fi, cell tower radiation).
- **Data Sources**: EPA AirNow, OpenAQ, NASA GIBS, FCC RF exposure maps, field sensors (Raspberry Pi + SDS011, MiCS6814, RF Explorer).
- **Biological Assays**: Partner with entomology labs to measure spiracle blockage, neural disruption, and immune response under controlled exposures.
- **Output**: Honeybee-specific NanoKarma hazard matrix (β_bee values), real-time threat dashboard visualizing hive micro-volumes (V_h) with pollutant/EMF heatmaps.

Adaptive Mitigation Algorithms

- **Task**: Extend Cybo-Air duty-cycle control law to prioritize honeybee neurorights by adjusting nanoprecipitation flux and airflow to maintain safe pollutant levels and negotiate with telecom infrastructure to reduce EMF exposure.
- **Methods**: Adjust `J_p,i` (nanoprecipitation flux) and `Q_i` (airflow) to maintain `C_j,p ≤ C_max_bee` for pollutants; negotiate with telecom infrastructure to reduce RF power density (`P_j^RF ≤ P_ref_bee`).
- **Biological Feedback**: Integrate hive weight sensors and bee counter data to dynamically adjust protection radius (`R_h`).
- **Output**: Rust crate `cyboair_beeguard` implementing mitigation algorithms; simulation using BEHAVE model to validate survival rate improvements.

Hardware Prototyping

- **Task**: Design modular Air-Globe nodes with electrostatic precipitator, MOF-coated mesh for VOCs/heavy metals, Faraday cage canopies for EMF shielding, and triboelectric nanogenerators for power.
- **Output**: CAD models, BOM for $200/node deployable unit, field test plan for 3 urban apiaries.

Phase 2: Governed AI & Rust Security Architecture (8–10 weeks)

Objectives

- Upgrade Cybo-Air's Rust backend to enforce role-based access control (RBAC), attribute-based access control (ABAC), and prompt-injection resistance.
- Implement a governance gateway that classifies users into tiers with augmented rights for verified stakeholders.

- Develop a generator–verifier pipeline for LLM actions to ensure compliance with Eibon rules and RBAC policies.

Key Tasks

Governance Gateway & RBAC Engine

- **Task**: Build a Rust-based policy enforcement layer (`cyboair_governance` crate) that classifies users into Eibon Superchairs, Verified Stakeholders, Trusted Staff, Guests, and Bots, with tiered access rights.
- **RBAC/ABAC Models**: Use Casbin-RS and Cedar policy language to support fine-grained permissions and real-time evaluation.
- **Output**: Rust trait `GovernedAction` with methods for authorization and audit logging; integration with Actix-Web/Axum for HTTP endpoints.

Prompt-Injection & Adversarial Defenses

- **Task**: Harden LLM interface against jailbreaks, data exfiltration, and control hijacking using structured prompts, input sanitization, and output filters.
- **Methods**: Separate system, policy, data, and user text slots; sanitize inputs using `validator`, `sanitizer`, and huginn crates; filter outputs for secrets and unauthorized commands.
- **Output**: Rust middleware crate `cyboair_llm_guard` with sanitization and verification functions; red-team corpus of 100+ adversarial prompts.

Augmented Rights & Language Detection

- **Task**: Train/fine-tune a classifier to detect stakeholder identity claims, adversarial patterns, and rights-asserting language.
- **Methods**: Use distilbert-model fine-tuned on labeled governance logs; implement rule-based fallback for low-confidence cases.
- **Output**: Rust FFI wrapper `cyboair_nlp` for classifier; tiered response policies based on user roles and intent.

Phase 3: Integration & Field Validation (6–8 weeks)

Objectives

- Deploy biological + governance systems in real-world urban apiaries.
- Validate performance through field trials and governance stress tests.
- Publish open-source tools and regulatory recommendations.

Key Tasks

Unified Rust Service

- **Task**: Combine bee protection algorithms, governance gateway, and LLM guards into a Dockerized Rust service with REST API and WebSocket for real-time monitoring.
- **Output**: Dockerized Rust service with audit trail (PostgreSQL) for all actions.

Field Deployment

- **Task**: Install 3 Air-Globe nodes in high-pollution apiaries; measure bee mortality, foraging efficiency, and neurological markers before/after intervention.
- **Metrics**: ≥30% reduction in bee mortality; ≥50% decrease in spiracle $PM_{2.5}$ deposition; ≥20% improvement in foraging efficiency.
- **Output**: Peer-reviewed preprint, open dataset of sensor logs + bee health metrics.

Governance Stress Test

- **Task**: Simulate adversarial attacks on the system, including prompt injection, role escalation, and data tampering.
- **Output**: Security report with false-positive/negative rates; mitigation patches.

Phase 4: Documentation & Open-Source Release (4 weeks)

Objectives

- Publish reproducible, governed tools for global use.
- Provide comprehensive technical and governance documentation.

Key Tasks

Technical Documentation

- **Task**: Write Rust crate docs, governance manual, and bee protection guide.
- **Output**: GitBook/MDBook site hosted on GitHub Pages.

Open-Source Release

- **Task**: Publish crates (`cyboair_beeguard`, `cyboair_governance`, `cyboair_llm_guard`) to crates.io; update Cybo-Air repo; release datasets to Zenodo.
- **Output**: Release blog post, community call for collaborators.

Policy Proposals

- **Task**: Draft regulatory recommendations for urban apiary EMF limits, pollutant standards, and AI governance.
- **Output**: Whitepaper submitted to EPA, FCC, and EU Pollinators Initiative.

Research Team Roles

Role	Skills Needed	Tools
Biological Lead	Entomology, Toxicology, Field Sensors	R, Python (Pandas), Bee Monitoring Kits
Rust Engineer	Systems Programming, Async, FFI	Rust, Tokio, PostgreSQL
AI Security Expert	LLM Red-Teaming, Prompt Engineering	Python (Transformers), Owasp Cheat Sheets
Governance Specialist	Policy Design, RBAC, Audit Trails	Rego (OPA), LaTeX
Field Technician	IoT Deployment, Data Logging	Raspberry Pi, QField, CAD Software

Budget Estimate

Category	Cost (USD)	Notes
Sensor Hardware	$5,000	10x PM/VOC/EMF nodes
Rust Development	$20,000	3 devs × 8 weeks
Field Trial	$10,000	Apiary rent, lab assays, travel
LLM Security Audit	$15,000	Red-team contract
Documentation	$5,000	Technical writing + GitBook
Total	**$55,000**	

Timeline

```
gantt
    title Cyconetic Air-Globe Research Plan
    dateFormat  YYYY-MM-DD
    section Phase 1: Biological System
    Pollutant Modeling       :a1, 2024-06-01, 30d
    EMF Threat Modeling       :a2, 2024-06-15, 30d
    Mitigation Algorithms    :a3, 2024-07-01, 30d
```

```
    Hardware Prototyping     :a4, 2024-07-15, 30d
    section Phase 2: Governance & Security
    RBAC Engine              :b1, 2024-08-01, 30d
    LLM Guards                :b2, 2024-08-15, 30d
    Language Classifier      :b3, 2024-09-01, 30d
    section Phase 3: Integration
    Unified Rust Service     :c1, 2024-09-15, 30d
    Field Deployment         :c2, 2024-10-01, 45d
    Stress Testing           :c3, 2024-10-15, 30d
    section Phase 4: Release
    Documentation            :d1, 2024-11-15, 30d
    Open-Source Publish      :d2, 2024-12-01, 15d
    Policy Proposals         :d3, 2024-12-15, 15d
```

Key Risks & Mitigations

Risk	Likelihood	Mitigation
Bee health metrics inconclusive	Medium	Partner with 3+ apiaries for redundancy
Rust governance bugs	High	Formal verification (e.g., Kani)
LLM jailbreaks	High	Weekly red-team drills
Regulatory pushback	Low	Pre-engage with EPA/FCC early
Hardware failures	Medium	Modular design for easy replacements

Success Metrics

1. **Biological**:
    - ≥30% reduction in bee mortality in treated hives vs. control.
    - ≥50% decrease in spiracle $PM_{2.5}$ deposition (microscopy).
    - ≥20% improvement in foraging efficiency (pollen weight).
2. **Technical**:
    - ≤1% false-positive rate in LLM prompt-injection blocks.
    - ≤100ms latency for governance authorization checks.
    - 100% audit compliance (no unauthorized qpudatashard access).
3. **Governance**:
    - Adoption by 2+ cities within 12 months.
    - Cited in 1+ policy proposal (e.g., EU Pollinators Initiative).

Next Steps for the Researcher

1. **Literature Review**:
    - Prioritize papers on bee neurology + EMF, urban air quality + pollinators, LLM security and red teaming.

2. **Stakeholder Engagement**:
    - Contact urban apiaries, telecom regulators, Rust security auditors, and Eibon governance experts.
3. **Prototype Development**:
    - Start with Rust CLI for `cyboair_beeguard` and Jupyter notebook for bee hazard modeling.
4. **Field Site Selection**:
    - Target cities with high pollution/EMF density and supportive regulators (e.g., Amsterdam, Portland).

This plan ensures biological efficacy, digital security, and governance integrity in a single, open-source system.