

Agentes de IA para buques inteligentes

Prototipos de IA agéntica para la guerra electrónica en escenarios navales



Agente de vulnerabilidad

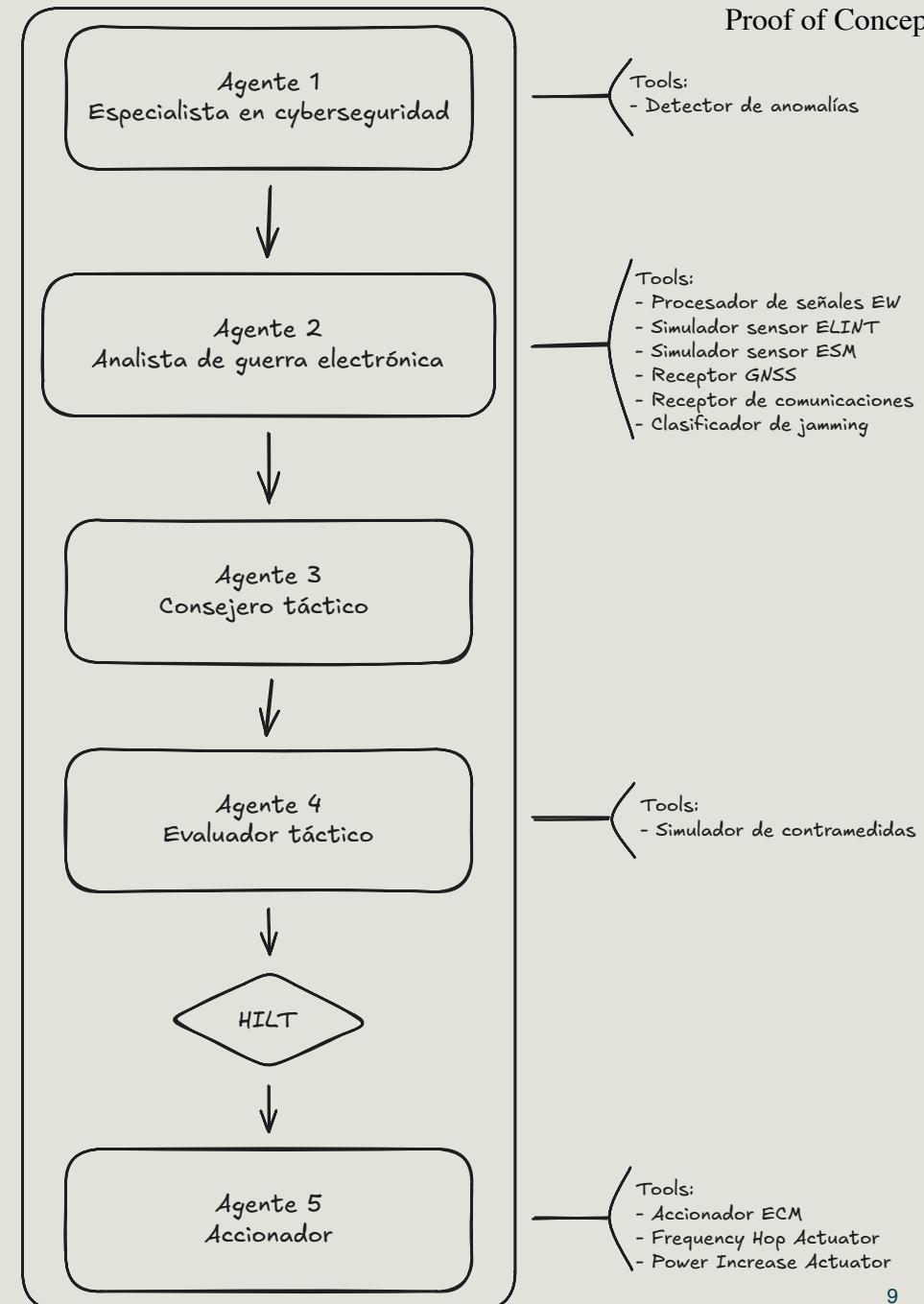
Vulnerabilidad: Responder ante un ataque

- **Contexto:** Una unidad hostil lanza un ataque de interferencia sobre el sistema de comunicaciones del buque.
- **Agente 1:** Detecta anomalías en el tráfico de red.
- **Agente 2:** Identifica la fuente de jamming y clasifica el tipo de señal.
- **Agente 3:** Propone tres planes de acción diferentes
- **HILT:** El oficial al responsable escoge el plan entre los propuestos
- **Agente 4:** Ejecuta la inferencia inversa y bloquea la señal enemiga



Agentes de IA
para buques
inteligentes

Prototipos de IA agéntica para la guerra electrónica en
escenarios navales



Agente de vulnerabilidad

Fwk: CrewAI

Input: Anomalías en tráfico de red (paquetes perdidos, incremento de latencia, degradación ancho de banda, etc) y herramientas de jamming enemigas.

Pestañas:

- **Network Anomalies:** Identificación de anomalías en las comunicaciones
- **Jamming Classification:** Fuentes del ataque
- **Proposed Plans:** Tres planes propuestos
- **Execution:** El plan escogido por el HILT

Status

MISSION COMPLETE
Plan 'UAV Kinetic Neutralization' executed successfully.

Assessment Reports

Network Anomalies Jamming Classification Proposed Plans Execution

COUNTERMEASURE EXECUTION REPORT

Selected Plan: UAV Kinetic Neutralization
Plan ID: PLAN-002

Naval Vulnerability Agent

Electronic Warfare Attack Response System

Multi-agent system for detecting jamming attacks, classifying sources, proposing countermeasure plans, and executing human-selected responses.

Quick Start

Select Scenario
Choose a predefined attack scenario
Scenario 2: Spot Jamming (Critical)

Load Scenario

Attack Input

Attack Data (JSON)

```
power_level: 62.0,
"jamming_type": "spot",
"bandwidth_mhz": 5.0,
"affected_systems": [
  "datalink",
  "fire_control"
],
"bearing_degrees": 135.0,
"range_km": 18.2
],
"network_anomalies": {
  "packet_loss": 85,
  "latency_increase": 650,
  "corrupted_frames": 340,
  "connection_drops": 12,
  "bandwidth_degradation_percent": 90
},
"threat_level": "critical",
"operational_impact": "Fire control datalink completely disrupted - immediate response required"
}
```

Run Assessment

Status

Assessment Reports

Network Anomalies Jamming Classification Proposed Plans Execution

Run an assessment to see results...

Human In The Loop - Select Plan to Execute

Plan 1 Plan 2 Plan 3

Usage Instructions

1. Select a Scenario or enter custom attack data in JSON format
2. Click Run Assessment to analyze the attack and generate 3 countermeasure plans
3. Review the Plans in the "Proposed Plans" tab
4. Select a Plan by clicking one of the buttons above
5. View Execution results in the "Execution" tab

Attack Data Format

Agente de vulnerabilidad - Especialista en ciberseguridad

Para cumplir su objetivo, los agentes llaman a distintas **Agent Tools** que hemos definido.

El agente “**Cybersecurity Network Analyst**” (Agente 1: Especialista en Ciberseguridad) detecta las anomalías con la herramienta “**Network Anomaly Detector**”.

```

  Agent: Cybersecurity Network Analyst
Thought: Thought: I will use the Network Anomaly Detector tool to analyze the provided attack data and detect network anomalies caused by electronic warfare.
Using Tool: Network Anomaly Detector

-----[Tool Output]-----
NETWORK ANOMALY DETECTION REPORT
Detection Time: 2025-10-21T15:45:00Z
Severity Level: CRITICAL
Analysis Status: COMPLETE

DETECTED ANOMALIES:
- Packet Loss: 85% △ CRITICAL
- Latency Increase: +650 ms △ CRITICAL
- Corrupted Frames: 340 △ HIGH
- Connection Drops: 12 △ CRITICAL
- Bandwidth Degradation: 90% △

AFFECTED SERVICES:
x Voice Communications (VoIP)
x Video Feeds (ISR)
x Real-time Tactical Datalink
x Command & Control Systems
x Sensor Data Fusion
x Fire Control Systems

ANOMALY CHARACTERISTICS:
Attack Pattern: Aggressive jamming (complete disruption)
Network Layer: Physical/Data Link Layer (RF interference)
Traffic Impact: 87%

CORRELATION ANALYSIS:
Correlation with RF jamming: CONFIRMED - 1 source(s) detected
- Source J-002: spot jamming at 1090.00 MHz

ASSESSMENT:
Network communications are severely compromised. Mission-critical systems experiencing catastrophic degradation.
Immediate countermeasures required to restore operational capability.

IMMEDIATE ACTIONS REQUIRED:
- Switch to backup SATCOM channels immediately
- Activate frequency hopping on all tactical links
- Increase transmission power (burn-through attempt)
- Locate and neutralize jamming source with UAV
- Implement EMCON procedures for non-essential systems

CONCLUSION: Network under electronic attack - CRITICAL severity
R...

```

Assessment Reports

- [Network Anomalies](#)
- [Jamming Classification](#)
- [Proposed Plans](#)
- [Execution](#)

NETWORK ANOMALY DETECTION REPORT Detection Time: 2025-10-21T15:45:00Z Severity Level: CRITICAL Analysis Status: COMPLETE

DETECTED ANOMALIES: • Packet Loss: 85% △ CRITICAL • Latency Increase: +650 ms △ CRITICAL • Corrupted Frames: 340 △ HIGH • Connection Drops: 12 △ CRITICAL • Bandwidth Degradation: 90% △

AFFECTED SERVICES: X Voice Communications (VoIP) X Video Feeds (ISR) X Real-time Tactical Datalink X Command & Control Systems X Sensor Data Fusion X Fire Control Systems

ANOMALY CHARACTERISTICS: Attack Pattern: Aggressive jamming (complete disruption) Network Layer: Physical/Data Link Layer (RF interference) Traffic Impact: 87%

CORRELATION ANALYSIS: Correlation with RF jamming: CONFIRMED - 1 source(s) detected → Source J-002: spot jamming at 1090.00 MHz

ASSESSMENT: Network communications are severely compromised. Mission-critical systems experiencing catastrophic degradation. Immediate countermeasures required to restore operational capability.

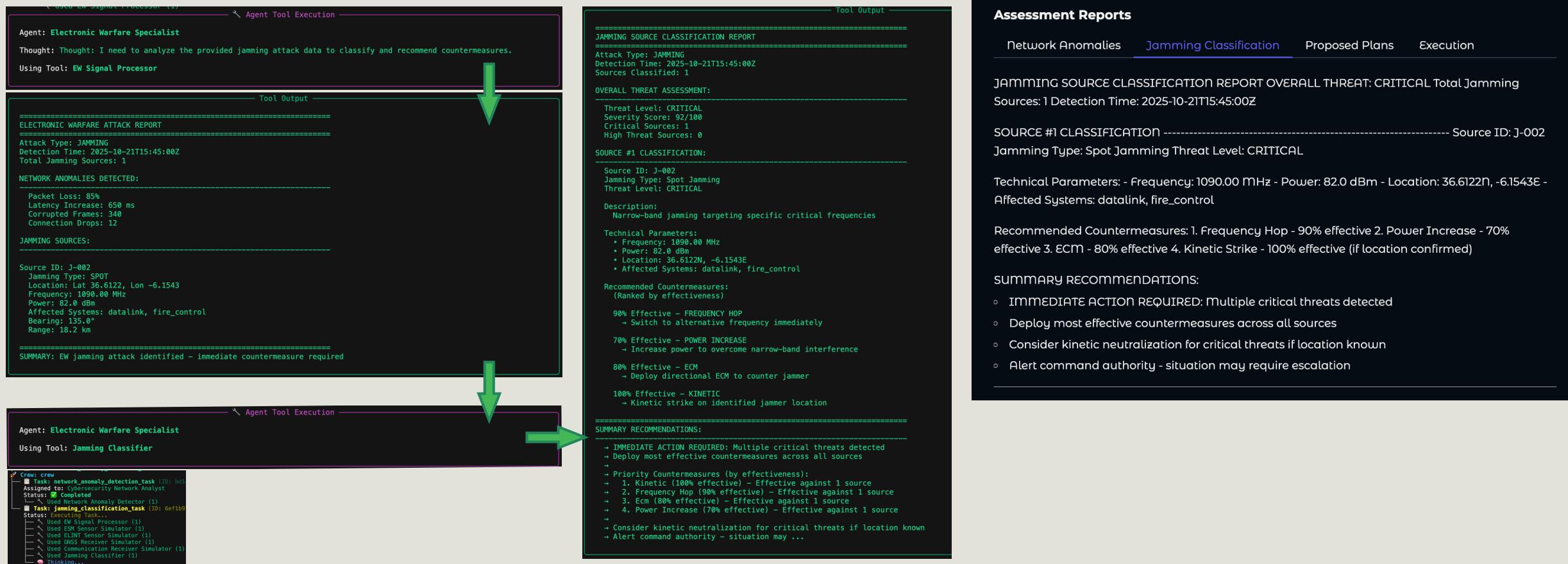
IMMEDIATE ACTIONS REQUIRED: → Switch to backup SATCOM channels immediately → Activate frequency hopping on all tactical links → Increase transmission power (burn-through attempt) → Locate and neutralize jamming source with UAV → Implement EMCON procedures for non-essential systems

CONCLUSION: Network under electronic attack - CRITICAL severity Recommend immediate countermeasure evaluation

Agente de vulnerabilidad - Analista de Guerra Electrónica

Para cumplir su objetivo, los agentes llaman a distintas **Agent Tools** que hemos definido.

Una vez el sistema identifica que está bajo ataque electrónico, el agente “**Electronic Warfare Specialist**” (Agente 2: Analista de Guerra Electrónica) clasifica el tipo de ataque con la herramienta “**EW Signal Processor**”. En el ejemplo se encuentras un ataque de jamming por lo que el agente llama a “**Jamming Classifier**” para identificar las fuentes de ataque y sus parámetros técnicos.



Agente de vulnerabilidad - Consejero y Evaluador Tácticos

Para cumplir su objetivo, los agentes llaman a distintas **Agent Tools** que hemos definido.

Con toda la información recolectada y procesada, el “**Tactical Response Planner**” (Agente 3: Consejero Táctico) genera tres contramedidas distintas para el ataque recibido. Cada uno de los tres planes tiene una filosofía diferente. Los tres planes definidos son luego valorados por el “**Plan Evaluator and Validator**” (Agente 4: Evaluador Táctico), que determina su viabilidad simulando cada uno de ellos con la herramienta “**Countermeasure Simulator**”. Esto se hace una vez por plan.

The diagram illustrates the workflow between three main components:

- Agent Final Answer:** Shows the JSON output of the "Tactical Response Planner". It includes sections for "Final Answer", "plans" (containing three plans for "PLAN-001" through "PLAN-003"), "PROS", and "CONS". A green arrow points from this screen to the next one.
- Agent Tool Execution:** Shows the "Plan Evaluator and Validator" tool. It displays a "Thought" message about evaluating plans using the Countermeasure Simulator, and a "Tool Output" section titled "COUNTERMEASURE SIMULATION REPORT". This report details the simulation of three countermeasures (Ecm, Power Increase, Frequency Hopping) against target J-002, with overall effectiveness of 57.5%.
- Status:** Shows the "Assessment Reports" screen. It indicates "ASSESSMENT COMPLETE - AWAITING PLAN SELECTION" and provides a summary of the three proposed plans, each with its own JSON details.

Uno de los planes propuesto por Agente 3

```

Agent: Tactical Response Planner
Final Answer:
```
{
 "plans": [
 {
 "Plan ID": "PLAN-001",
 "Plan Name": "Aggressive Electronic Warfare",
 "Countermeasures": [
 {
 "Type": "ECM",
 "Target": "J-002",
 "Params": {
 "frequency": "1090.00 MHz",
 "power": "85 dBm",
 "direction": "towards jamming source"
 },
 "Estimated Effectiveness": 80
 },
 {
 "Type": "Power Increase",
 "Target": "J-002",
 "Params": {
 "power": "100 dBm"
 },
 "Estimated Effectiveness": 70
 },
 {
 "Type": "Frequency Hopping",
 "Target": "J-002",
 "Params": {
 "channel frequency": "alternate frequencies"
 },
 "Estimated Effectiveness": 90
 }
],
 "Overall Effectiveness": 80,
 "Execution Time": 30,
 "Resource Cost": "HIGH",
 "PROS": [
 "High potential to restore communications quickly.",
 "Aggressive approach targets the enemy directly.",
 "Flexible to use multiple electronic countermeasures."
],
 "CONS": [
 "Requires significant energy and resources.",
 "Could escalate electronic conflict with the enemy.",
 "Possible collateral effects on own electronic systems."
]
 },
 {
 "Plan ID": "PLAN-002",
 "Plan Name": "Kinetic Neutralization",
 "Countermeasures": [
 ...
]
 }
]
}
```

```

Agente de vulnerabilidad - HILT y Accionador

Para cumplir su objetivo, los agentes llaman a distintas **Agent Tools** que hemos definido.

Finalmente, el oficial al mando debe escoger uno de los tres planes propuesto y el “**Countermeasure Execution Officer**” (Agente 5: Accionador) lo llevará a cabo empleando cualquier de las actuator tools como “**ECM Actuator**”, “**Power Increase Actuator**”, “**Frequency Hop Actuator**”, etc

