

Agentes de IA para buques inteligentes

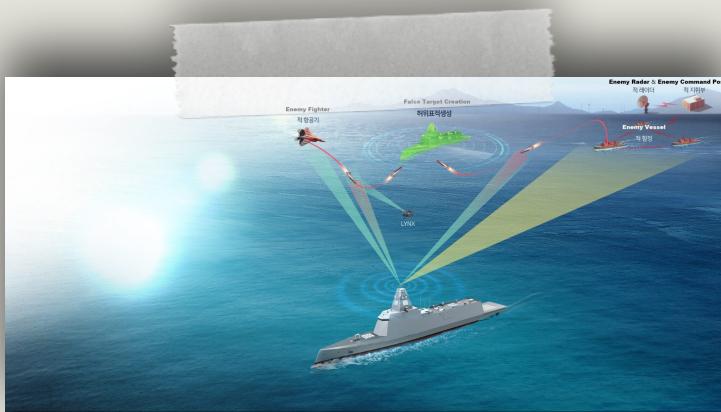
Prototipos de IA agéntica para la guerra electrónica en escenarios navales



Agente de susceptibilidad

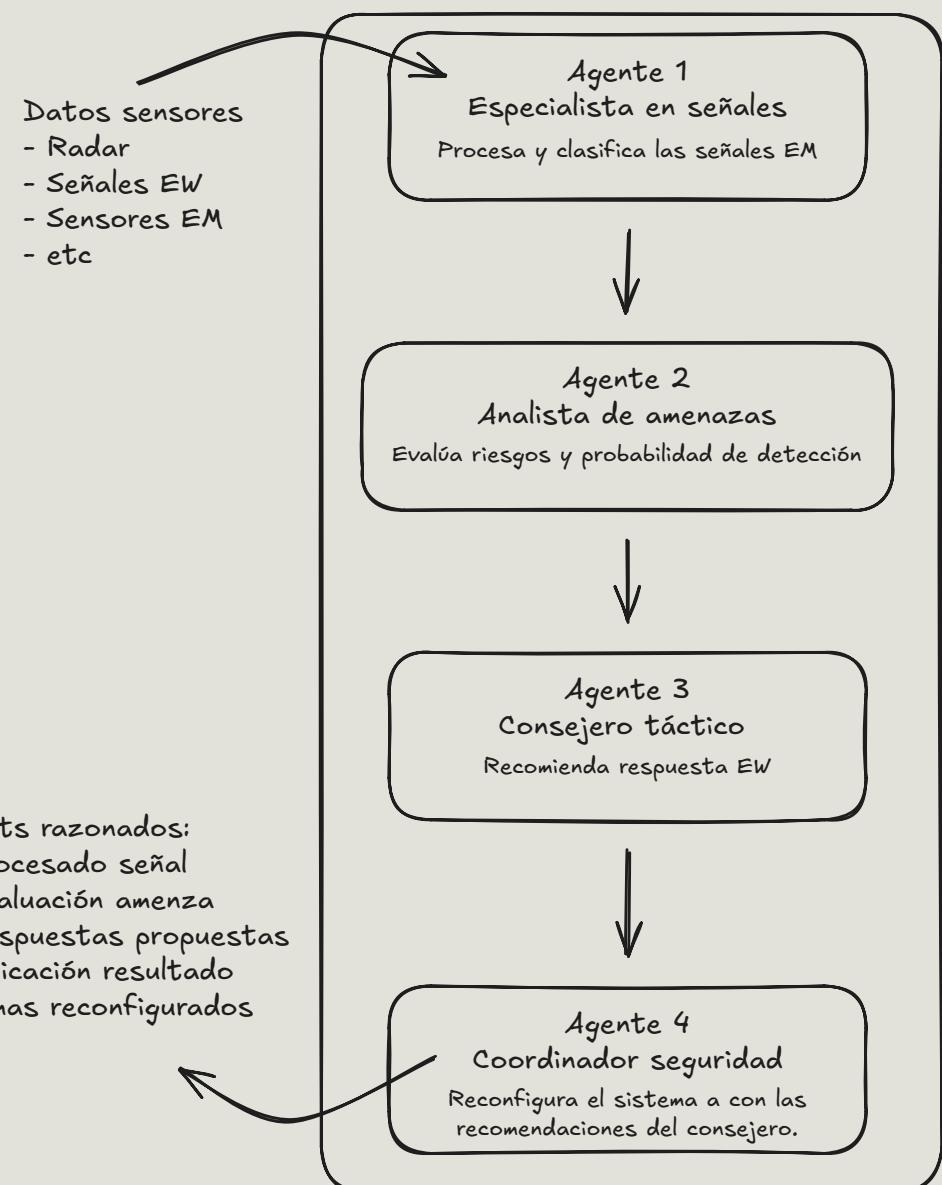
Susceptibilidad: **Evitar ser atacado**

- **Contexto:** El buque navega en una zona de alta amenaza electromagnética. Los sensores detectan emisiones radar de largo alcance.
- **Agente 1:** Identifica patrones de búsqueda de un sistema de armas enemigo.
- **Agente 2:** Predice la probabilidad de detección en función de la firma EM.
- **Agente 3:** Recomienda modificaciones el perfil de emisiones.
- **Agente 4:** Reconfigura automáticamente los canales de comunicación para evitar exposición.



Agentes de IA
para buques
inteligentes

Prototipos de IA agéntica para la guerra electrónica en escenarios navales



Agente de susceptibilidad

Fwk: CrewAI

Input: Señales electrónicas enemigas detectadas por nuestros sensores de EW.

Pestañas:

- **Signal Intelligence:** Describe los elementos de EW enemigos detectados
- **Threat Assessment:** Evalúa el riesgo de ser detectados teniendo en cuenta los sensores enemigos y la firma electrónica propia.
- **EW Response:** Detalla las recomendaciones para una respuesta táctica para evitar la detección
- **Communications:** Reporte de la reconfiguración del perfil de emisiones del buque. Se sigue la recomendación de la EW response.

The screenshot displays the 'Naval Susceptibility Agent' interface for the 'Electromagnetic Warfare Threat Assessment System'. The interface is dark-themed with blue and white text.

Quick Start: A section for selecting a scenario or entering custom data. It shows a dropdown menu with 'Scenario 2: Medium Threat - Military Presence' selected. Below it is a 'Load Scenario' button.

Signal Input: A section for entering signal data in JSON format. The JSON code provided is:

```

{
  "sensor_type": "esm",
  "operational_mode": "normal",
  "detections": [
    {
      "emitter_id": "E-001",
      "emitter_type": "radar",
      "frequency_mhz": 2850.0,
      "power_dbm": 62.5,
      "bearing_degrees": 45.0,
      "range_km": 95.0,
      "classification": "Early Warning Radar"
    },
    {
      "emitter_id": "E-002",
      "emitter_type": "radar",
      "frequency_mhz": 8500.0,
      "power_dbm": 58.0,
      "bearing_degrees": 48.0,
      "range_km": 92.0,
      "classification": "Surface Search Radar"
    }
  ]
}

```

Active Ship Systems (comma-separated): A list of currently emitting systems: radar, communications, navigation_radar, datalink, iff

Status: Shows the system is initializing crew... at 10.0% completion. The status bar also shows 10.7/0.0s.

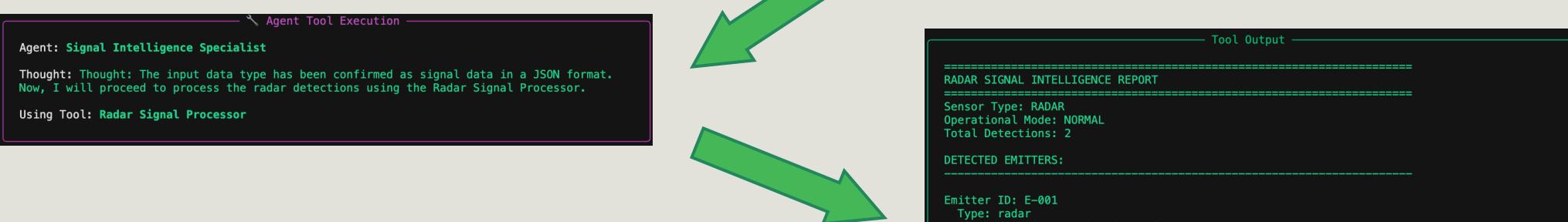
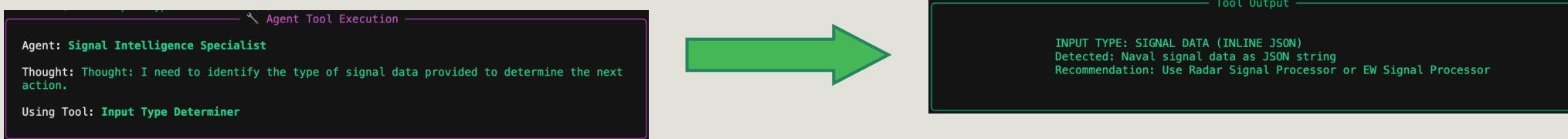
Assessment Reports: A tabbed section showing Signal Intelligence, Threat Assessment, EU Response, and Communications. The Signal Intelligence tab is active.

Usage Instructions: A numbered list of steps:
 1. Select a Scenario or enter custom signal data in JSON format.
 2. Specify Active Systems currently emitting from your ship.
 3. Click Run Assessment to process the electromagnetic environment.
 4. Review Reports in each tab for detailed analysis and recommendations.

Agente de susceptibilidad - Especialista en señales

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

El agente “**Signal Intelligence Specialist**” (Agente 1: Especialista en Señales) llama a la herramienta de “**Input Type Determiner**”, una vez determina que se trata de una señal de radar, llama a la custom tool “**Radar Signal Processor**”. Esta herramienta identifica las dos señales de radar enemigo (E-001 y E-002) y sus propiedades.



El agente de especialista en señales decide de manera autónoma a qué herramienta debe llamar en cada situación. Obsérvese el “Thought” en la caja “ Agent Tool Execution”.

Agente de susceptibilidad - Analista de Amenazas

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

El agente “**Threat Assessment Analyst**” (Agente 2: Analista de Amenazas) llama dos veces a la herramienta de “**Emitter Threat Lookup Tool**”, una por cada uno de las señales de radar enemigo detectadas.

```
Agent: Threat Assessment Analyst
Thought: Thought: I will query the threat database for each detected emitter to determine the threat levels.
Using Tool: Emitter Threat Lookup Tool
```



```
Tool Output
=====
EMITTER THREAT ASSESSMENT
=====
Emitter Type: VHF Marine Radio
Description: Unidentified emitter requiring further analysis

● THREAT LEVEL: MEDIUM
Threat Score: 60/100
Detection Probability: 60.0%

RECOMMENDED ACTION:
→ Increase vigilance – gather more intelligence

TACTICAL IMPLICATIONS:
• If detected by this emitter, expect engagement within detection range
• Higher threat scores indicate need for immediate electronic countermeasures
• Detection probability reflects likelihood of our ship being tracked
=====
```

```
Agent: Threat Assessment Analyst
Thought: To conduct a comprehensive threat assessment, I will first query the threat database regarding the detected electromagnetic emitters, E-001 and E-002.
**Emitter E-001: Navigation Radar**
Thought: I need to determine the threat level of E-001, which is a Navigation Radar.
Using Tool: Emitter Threat Lookup Tool
```



```
Tool Output
=====
EMITTER THREAT ASSESSMENT
=====
Emitter Type: Navigation Radar
Description: Standard maritime navigation radar

● THREAT LEVEL: LOW
Threat Score: 40/100
Detection Probability: 50.0%

RECOMMENDED ACTION:
→ Continue monitoring – no immediate action required

TACTICAL IMPLICATIONS:
• If detected by this emitter, expect engagement within detection range
• Higher threat scores indicate need for immediate electronic countermeasures
• Detection probability reflects likelihood of our ship being tracked
=====
```

El “**Emitter Threat Lookup Tool**” hace a una query a una base de datos de amenazas para evaluar el tipo de riesgo que puede conllevar.

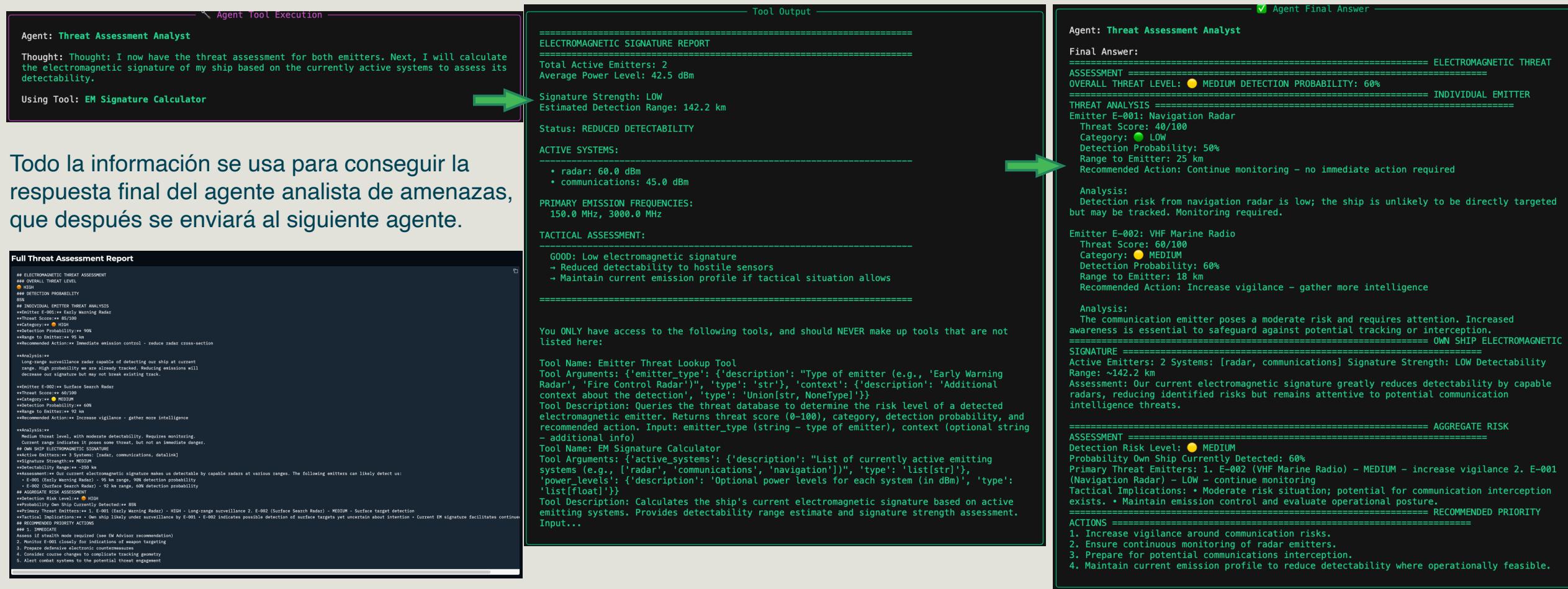
Para cada señal de EW enemiga asigna un nivel de amenaza y una probabilidad de detección.

También se discuten las implicaciones tácticas de una detección y sugiere recomendaciones de acción. Aunque el analista de amenazas no será el agente encargado de sugerir la repuesta final.

Agente de susceptibilidad - Analista de Amenazas

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

Una vez se han evaluado la amenazas con la “**Emitter Threat Lookup Tool**”, el agente “**Threat Assessment Analyst**” llama a la herramienta “**EM Signature Calculator**” para calcular la firma electrónica de nuestro buque basándose en los sistemas electrónicos activos.



Agente de susceptibilidad - Consejero táctico

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

El agente “**Electronic Warfare Tactical Advisor**” (Agente 3: Consejero Táctico) propone el plan de acción

Status

ASSESSMENT COMPLETED SUCCESSFULLY
All reports generated. Review each tab for detailed analysis.

Assessment Reports

- Signal Intelligence
- Threat Assessment
- EW Response**
- Communications

ELECTRONIC WARFARE RESPONSE RECOMMENDATION

RECOMMENDED ACTION

- ACTIVATE STEALTH MODE

THREAT JUSTIFICATION

Current threat level: HIGH Detection probability: 85% Primary concerns: Early Warning Radar (E-001), Surface Search Radar (E-002)

DETAILED RECOMMENDATION

STEALTH MODE ACTIVATION REQUIRED

Rationale: Given the current detection probability of 85%, there is a high risk that our ship is being tracked by E-001 (Early Warning Radar). The immediate activation of stealth mode is necessary to reduce our electromagnetic signature and minimize the likelihood of further detection or targeting. **Emission Control Level:** EMCON Charlie (full silence) **Systems to Secure:** Non-essential radar

- Non-essential communications
- Other high-signature emitters

Essential Systems to Maintain:

- Critical command/control channels
- Minimum sensors for situational awareness

Countermeasure Preparation:

- Ready chaff/decoy systems in anticipation of potential threats
- Prepare active jamming in case of escalated threats
- Alert combat systems crew to stay vigilant and ready for potential engagement

TACTICAL GUIDANCE

Course/Speed Recommendations: Consider altering course to obscure radar profile and break tracking geometry. Maneuver to reduce speed and change course subtly to minimize radar signatures. **Sensor Employment:** Maintain passive sensor systems and limit active sensors to essential usage. Emphasize communications discipline to avoid unnecessary emissions. **Communication Security:** Adjust communication protocols to ensure critical messages only are transmitted, enhancing operational security. Recommend signal reconfiguration if contact communications escalate, which will trigger the Comm Coordinator.

DECISION POINTS

Reassess situation if:

- Detection of fire control radar activity from E-001
- Decrease in range to E-001 below 85 km
- Any new CRITICAL threats are detected

BOTTOM LINE

Recommend immediate stealth mode activation due to high detection probability and risk of tracking by Early Warning Radar.

Status: EXECUTING ANSWER Agent Final Answer

Agent: Electronic Warfare Tactical Advisor

Final Answer:

```
=====
ELECTRONIC WARFARE
=====
RECOMMENDED ACTION: INCREASE READINESS
THREAT JUSTIFICATION: Current threat level: MEDIUM Detection probability: 60% Primary concerns: VHF Marine Radio (E-002), Navigation Radar (E-001)
=====
DETAILED RECOMMENDATION
=====
**CURRENT POSTURE ACCEPTABLE**
Rationale: The threat level is assessed as MEDIUM with a detection probability of 60%. While there are risks associated with the VHF Marine Radio and navigation radar, the ship maintains a low signature profile that decreases overall detectability. Continued monitoring and increased vigilance around these emitters is essential to address potential communication interception or tracking.

Monitoring Requirements:
- Continue tracking VHF Marine Radio (E-002) to detect any increase in threat level.
- Continuously monitor Navigation Radar (E-001) as an additional precaution.
- Maintain vigilance for any changes in operational environment or detected emitters.

Trigger Points for Stealth Mode:
- Detection of fire control radar activity.
- Detection probability exceeding 80%.
- New CRITICAL threats detected.

=====
TACTICAL GUIDANCE
=====
Course/Speed Recommendations: Consider minor course changes and speed adjustments to complicate tracking if necessary; maintain a course that maximizes distance from known emitters.
Sensor Employment: Utilize passive sensors primarily, only activating active sensors when required to minimize detectability. Use radar sparingly and only as necessary.
Communication Security: Review communication protocols to minimize the risk of interception. Recommended discussions with the Communication Coordinator to adjust transmission protocols as needed.

=====
DECISION POINTS
=====
Reassess situation if:
- Detection probability for VHF Marine Radio increases above 70%.
- New threat intelligence is received indicating high-risk emitters in proximity.
- Any detected increase in emissions from E-001 or E-002 yielding tactical significance.

=====
BOTTOM LINE
=====
Maintain current posture, continue monitoring.
```

Agente de susceptibilidad - Consejero táctico

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

Finalmente, con las recomendaciones del “**Electronic Warfare Tactical Advisor**”, el agente “**Communications Security Coordinator**” (Agente 4: Coordinador de seguridad) llama a la herramienta “**Communications Reconfiguration Tool**” para que modifique el perfil del comunicaciones del buque y pase al modo sigilo.

Assessment Reports

- Signal Intelligence
- Threat Assessment
- EW Response
- Communications**

COMMUNICATIONS RECONFIGURATION REPORT

STEALTH MODE

ACTIVE Threat Level: HIGH Reconfiguration Completed: [Timestamp]

CHANGES IMPLEMENTED

- ✓ Frequency hopping enabled on all priority channels
- ✓ Enhanced encryption activated
- ✓ Power reduction applied (if threat CRITICAL/HIGH)
- ✓ Non-essential channels secured

ACTIVE COMMUNICATION CHANNELS

- SATCOM Primary: 7500-8500 MHz - OPERATIONAL
- UHF Tactical: 225-400 MHz - OPERATIONAL (if threat ≤ HIGH)
- Datalink Command: 960-1215 MHz - OPERATIONAL

SECURED CHANNELS

- VHF Primary: SECURED
- HF Long Range: SECURED

OPERATIONAL IMPACT

- Command and control: MAINTAINED
- Tactical coordination: MAINTAINED
- Long-range communications: SECURED

COORDINATION ACTIONS REQUIRED

- Notify task force of frequency changes
- Update crypto keys per EMCON procedures
- Confirm backup comm procedures with adjacent units
- Test priority channel connectivity

Agent Tool Execution

Agent: **Communications Security Coordinator**

Thought: I need to proceed with the communication system reconfiguration since the EW Advisor recommended activating stealth mode due to the high threat level.

Using Tool: **Communications Reconfiguration Tool**

Tool Output

```
=====
COMMUNICATIONS RECONFIGURATION - STEALTH MODE ACTIVE
=====
```

Threat Level: HIGH
Channels Reconfigured: 3/6

STEALTH CONFIGURATION:

- Frequency Hopping: ENABLED
- Power Reduction: ACTIVE
- Encryption Level: ENHANCED
- Emission Control: ACTIVE

ACTIVE PRIORITY CHANNELS:

- UHF_Tactical: 225-400 MHz
- SATCOM_Primary: 7500-8500 MHz
- Datalink_Command: 960-1215 MHz

TACTICAL IMPLICATIONS:

HIGH THREAT - Tactical communications maintained

- Non-essential channels SECURED
- Frequency hopping active on all channels
- Reduced power to minimize detection
- Enhanced encryption deployed

OPERATIONAL NOTES:

- Coordinate frequency changes with task force
- Monitor for communication degradation
- Prepare backup channels if primary compromised
- Update crypto keys per EMCON procedures

STATUS: Communications reconfigured for stealth operations

Con esto se modificarían de manera automática la comunicaciones del buque para evitar la detección. Sin intervención humana.