DEFENCE AND SPACE
Cyber

Guerra de la Información en el Ciberespacio

Capacidades técnicas y operativas integradas de extremo a extremo

AIRBUS

Hacer frente a las campañas de información

Basándonos en nuestra experiencia en el ámbito de la inteligencia y la ciberguerra defensiva, así como en el trabajo realizado desde 2021 sobre la guerra de ciber influencia, ofrecemos **un nuevo enfoque para automatizar la gestión de incidentes en el campo de la información**, limitando al mismo tiempo los costes y plazos específicos de implementación.

Al combinar la experiencia de Airbus en ciberseguridad y defensa, podemos proporcionar **capacidades técnicas y operativas integradas de extremo a extremo** que cumplen con la doctrina militar de 2021 sobre la Guerra de la Información del Ciberespacio.

UNA SOLUCIÓN COMPLETA Y MODULAR

- **Recopilación integral de datos** a través de nuestros socios
- **Procesamiento masivo** de datos y capacidades de IA
- **Análisis en profundidad** y detección de comportamiento
- **Explotación** mediante herramientas soberanas de respuesta a incidentes
- **Formación** utilizando herramientas realistas de simulación de la infoesfera

Nuestras capacidades en guerra de la información ciberespacial se basan en nuestra experiencia interna y en componentes soberanos, así como en un **ecosistema completo de socios franceses y europeos** que gestionamos.

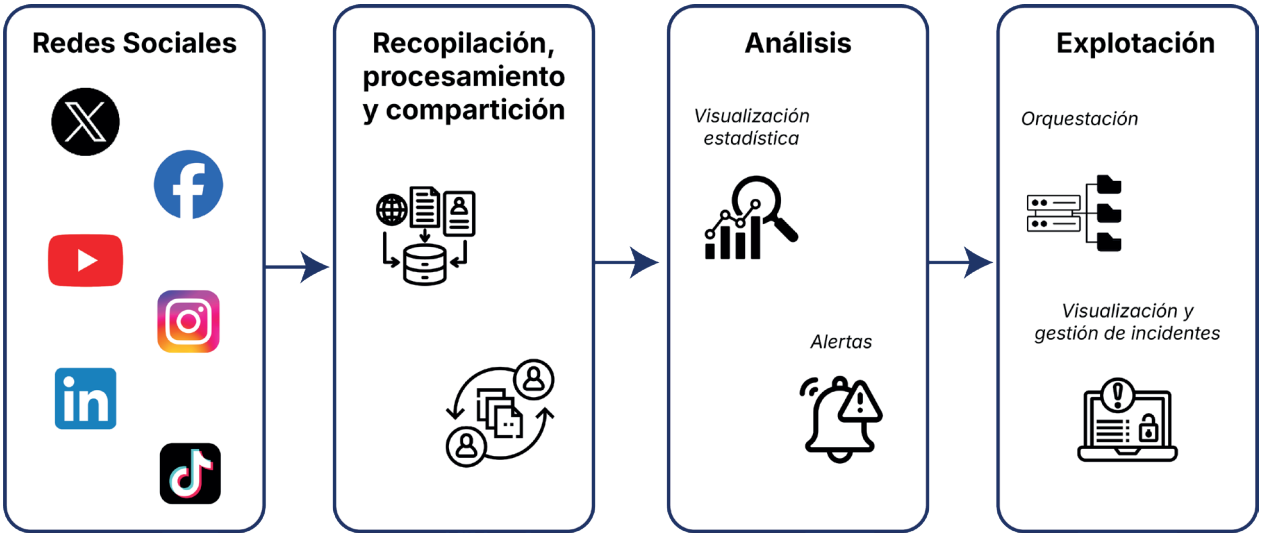
Nuestras soluciones pueden desplegarse de forma progresiva para apoyar el desarrollo de habilidades en este campo.

Cadena de detección automatizada

Integramos todos los componentes de la cadena de valor de la guerra de la información ciberespacial:

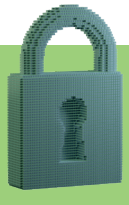
- Recopilación e investigación de contenidos en redes sociales
- Captación e informe de tendencias
- Análisis de la fiabilidad de las fuentes de información
- Investigación de cuentas y perfiles, caracterización de la huella digital de las personas
- Análisis de inteligencia multifuente
- Herramientas de detección de amenazas, orquestación, gestión de incidentes y remediación adaptadas a las necesidades de la Defensa de Redes Informáticas

Este enfoque nos permite proporcionar un conjunto de herramientas fácilmente actualizable y constantemente a la vanguardia de la tecnología.



Soluciones soberanas

Ofrecemos capacidades operativas que abarcan la recopilación, el análisis y la explotación de datos. Al final de la cadena, se puede compartir un informe de situación con el centro de Mando y Control del Ciberespacio.



Formación en gestión de crisis de información

Con el auge de las **redes sociales** y el rápido desarrollo de la **inteligencia artificial**, el entorno de la información es cada vez más el objetivo de **campañas de desinformación** y **brechas de datos**. El análisis humano ya no es suficiente para contrarrestar la difusión masiva de información manipulada, especialmente a través de tecnologías como los "**deep fakes**" (bulos).

Ante estas nuevas amenazas, la **gestión de crisis de información** se ha vuelto esencial. El uso de **herramientas tecnológicas** capaces de detectar rápidamente estas **amenazas híbridas** es crucial, combinado con el análisis humano para permitir una **respuesta eficaz** tanto en el ámbito civil como en el militar.

Módulo de formación COGNITIO

Ofrecemos un **módulo de formación en gestión de crisis de información**, que incluye una **simulación de la infoesfera** diseñada para facilitar el **entrenamiento** en la **detección y respuesta a campañas de influencia digital**.

Este módulo abarca tres objetivos principales:

- **Prevención:** Concienciar a los empleados sobre las campañas de desinformación, detectar amenazas híbridas en una fase temprana y limitar su aparición
- **Gestión de crisis:** Detectar y evaluar las amenazas rápidamente, escalar las alertas de seguridad e implementar contramedidas en tiempo real
- **Evaluación:** Evaluar la eficacia de la gestión de crisis e identificar posibles áreas de mejora, tanto en términos de formación como en los aspectos organizativos del sistema de gestión de crisis

Formación inmersiva

El módulo Cognitio, integrado directamente en nuestra solución CyberRange, fue diseñado para **apoyar a los analistas de ciberseguridad a anticipar, detectar y contrarrestar** campañas de desinformación.

Cognitio ofrece:

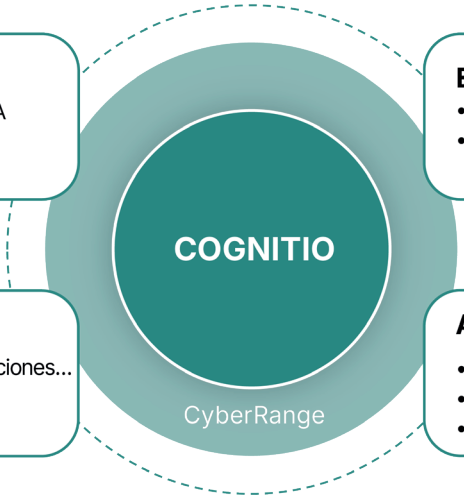
- Un **entorno inmersivo**
- **Generación automatizada de contenido** mediante **IA generativa**
- **Generación de actividad simulada impulsada por IA** (o simulación de entornos vivos)
- **Escenarios bajo demanda** en solo unos pocos clics
- Conjuntos de datos que cumplen con el **RGPD**

Generación de contenido

- Miles de perfiles y contenidos generados por IA
- Miles de interacciones impulsadas por IA
- Creación de campañas de influencers con IA

Entrenamiento / Formación

- Equipos Rojo, Azul y Gris (Red, Blue y Grey teams)
- Escenarios bajo demanda

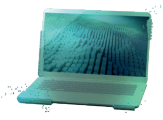


Visualización

- Monitorización, estadísticas, gráficos, configuraciones...
- Creación de avatares y publicaciones
- Acceso a través de PC y smartphone

Alojamiento de una infoesfera viva

- Redes sociales
- Sitios web de noticias
- Mensajería instantánea



Varios ejercicios realizados por el Ministerio de las Fuerzas Armadas de Francia se han beneficiado de COGNITIO como parte de una prestación de servicios. Todos los comentarios han sido positivos.

Caja de herramientas europea para la guerra ciberespacial y de la información (EUCINF)

Airbus Defence and Space coordina el p**royecto EUCINF***, cuyo objetivo es abordar los **desafíos de la guerra cognitiva** utilizando tecnologías de vanguardia basadas en **IA**.

El objetivo es **detectar y contrarrestar la desinformación** tan pronto como se publique, mejorando significativamente las **capacidades europeas de guerra de la información** mediante el desarrollo de una biblioteca compartida que reúna productos y software innovadores en este ámbito.

Airbus coordina este **proyecto de la Comisión Europea** con el apoyo de **ocho Estados miembros de la UE y el CIDCC** (Centro de Coordinación del Dominio Ciberespacial y de la Información). El consorcio reúne a expertos de **12 países** y **22 socios** en Guerra de la Información, IA y ciberseguridad, incluyendo grandes empresas, pymes y universidades.

Este enfoque único ha permitido la entrega de una **plataforma experimental** y aplicaciones configurables que sirven como casos de uso para la guerra de la información tanto civil como militar.

Desarrollar escenarios realistas

- El proyecto EUCINF incluye tres escenarios operativos
- Se realizan estudios de casos específicos para satisfacer las necesidades de los **Ministerios de Defensa** participantes y de determinadas partes interesadas civiles, garantizando al mismo tiempo el **cumplimiento de las normativas aplicables y las expectativas sociales**
- Se desplegarán soluciones desarrolladas por uno o más socios para **detectar, evaluar y abordar** rápidamente las **amenazas,** notablemente mediante la automatización de procesos habilitada por la **inteligencia artificial y la interoperabilidad de las plataformas**.

EUCINF
EUROPEAN CYBER INFORMATION WARFARE TOOLBOX

European Commission

EUCINF demuestra su relevancia y eficacia a niveles **estratégico, operativo y táctico**, en el contexto de la **Guerra de la Información combinada con la Defensa de Redes Informáticas** tanto en el **ámbito civil como en el militar**.

** Cofinanciado por la Unión Europea. Sin embargo, las opiniones y puntos de vista expresados son exclusivamente los del autor o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de los mismos.*

Airbus Defence and Space
Francia, Alemania, Reino Unido, España

Este documento no tiene carácter contractual. Sujeto a modificación sin previo aviso. © 2026 Airbus Defence and Space. AIRBUS, su logo y los nombres de los productos son marcas registradas. Todos los derechos reservados.

cyber.airbus.com
contact.cybersecurity@airbus.com
@Airbus Defence and Space Cyber

AIRBUS