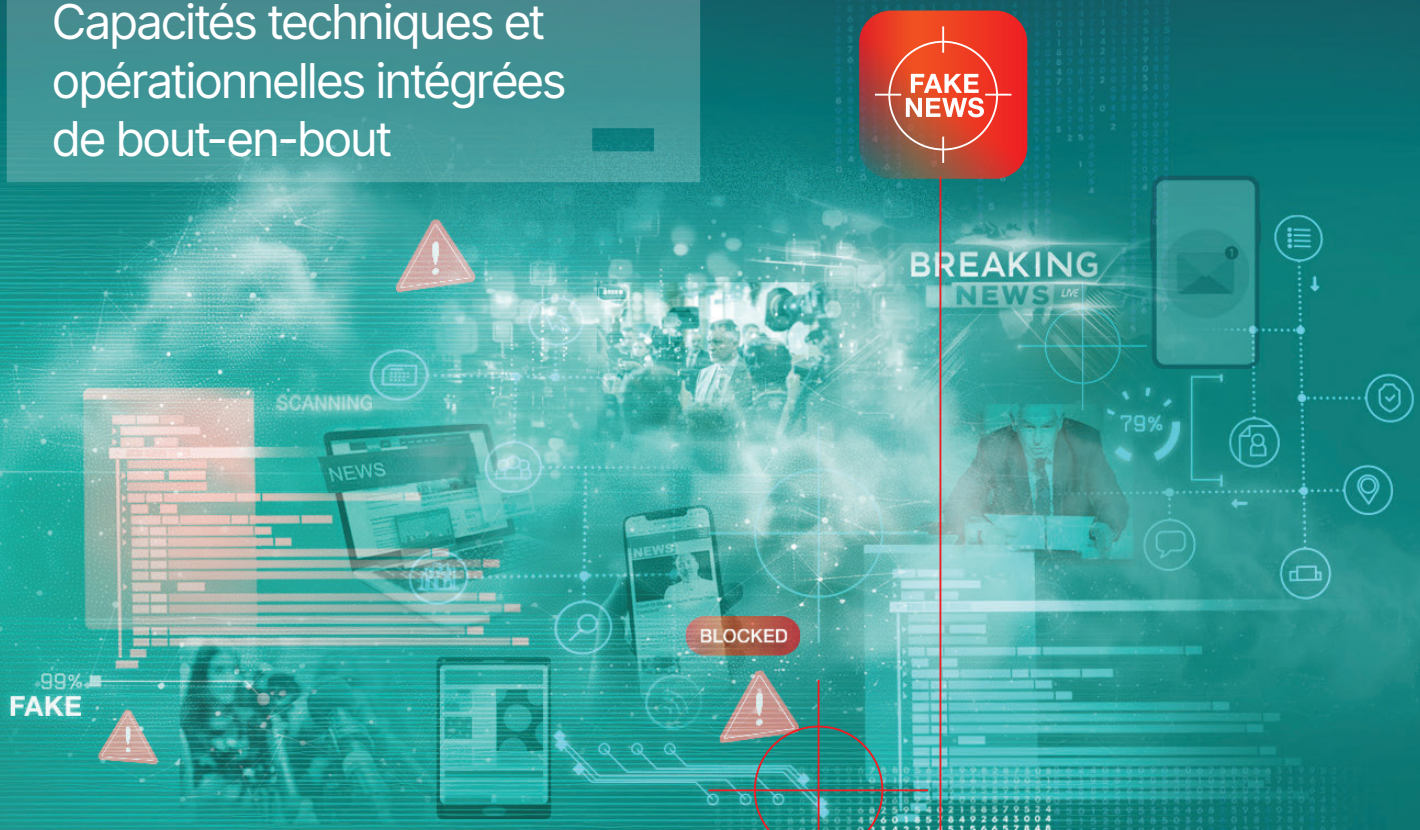
DEFENCE AND SPACE
Cyber

Lutte Informatique d'Influence (L2I)

Capacités techniques et opérationnelles intégrées de bout-en-bout



AIRBUS

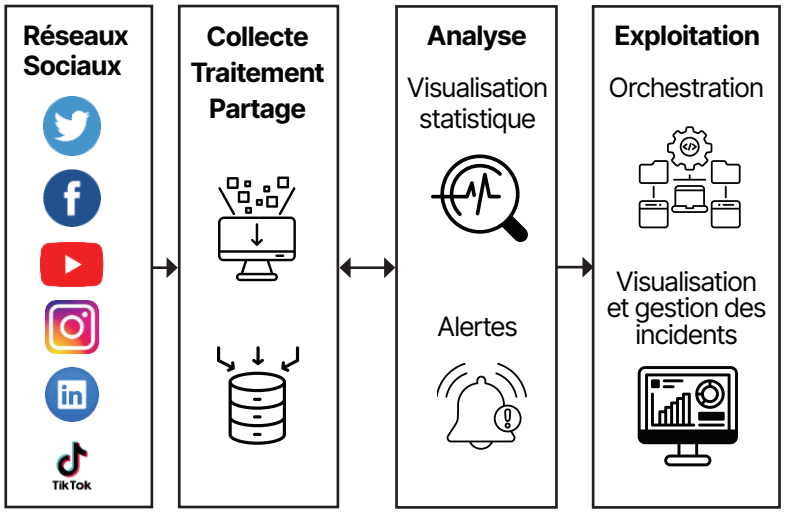
Lutter contre les campagnes informationnelles

Fort de notre expérience dans le domaine de la lutte informatique défensive, du renseignement, et des travaux menés depuis 2021 sur la lutte informatique d'influence, nous proposons **une nouvelle approche pour automatiser la gestion des incidents dans le champ informationnel** ; tout en limitant les coûts et délais de mise en œuvre spécifiques.
En combinant les expertises d'Airbus Intelligence et d'Airbus Cyber, nous fournissons des **capacités techniques et opérationnelles intégrées et de bout-en-bout** répondant à la doctrine militaire de Lutte Informatique d'Influence (L2I) 2021.

SOLUTION COMPLÈTE ET MODULAIRE

- **Collecte** exhaustive en s'appuyant sur nos partenaires
- **Traitement** en masse des données, capacités d'IA
- **Analyse** en profondeur et détection des comportements
- **Exploitation** via outils souverains de réponse à incident
- **Entrainement** via des outils d'animation d'infosphère réalistes

Nos capacités de Lutte Informatique d'Influence s'appuient sur notre expertise, nos composants souverains internes et un **écosystème complet de partenaires** que nous animons.
Nos solutions peuvent être déployées progressivement et accompagner une montée en compétence sur le sujet.



Des solutions souveraines

Nous proposons des capacités opérationnelles couvrant la collecte, l'analyse et l'exploitation des données.

En bout de chaîne, un rapport de situation est partageable avec le C2 Cyber.

CHAÎNE DE DÉTECTION AUTOMATISÉE

Nous intégrons l'ensemble des composants de la chaine de valeur L2I :

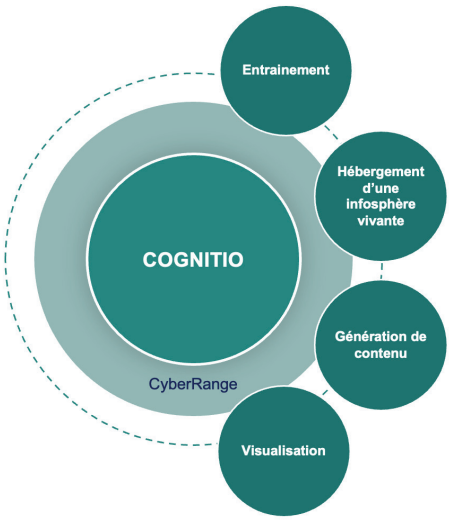
- Collecte et investigation de contenus sur les réseaux sociaux
- Collecte et rapports sur tendances
- Analyse de la fiabilité des sources d'information
- Investigation sur comptes et profils, caractérisation de l'empreinte numérique des personnes
- Analyse de renseignement multi-sources
- Outils de détection de la menace, d'orchestration, de gestion d'incidents et de remédiation adaptés de la Lutte Informatique Défensive

Ce positionnement nous permet de fournir une boîte à outils facilement évolutive et constamment à l'état-de-l'art.

MODULE COGNITIO - CYBERRANGE

Plateforme d'entraînement à la L2i permettant de simuler une infosphère qui facilite l'entraînement à la détection et à la contre-mesure de campagnes d'influences numériques.

- Environnement immersif
- Génération de contenu, propulsée par l'IA
- Génération de vie, propulsée par l'IA
- Scénarios à la demande en quelques cliques
- Jeux de données RGPD compatibles



Plusieurs exercices du Ministère des Armées ont pu bénéficier de COGNITIO dans le cadre d'une prestation de service, avec des retours très positifs.

Airbus Defence and Space
France, Allemagne Royaume-Uni, Espagne

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

AIRBUS