DEFENCE AND SPACE
Cyber

# Cyber-Informationskriegsführung

## Integrierte technische und operative End-to-End-Fähigkeiten


AIRBUS

# Bekämpfung von Informationskampagnen

Aufbauend auf unserer Erfahrung im Bereich der defensiven Cyberkriegsführung und Informationsbeschaffung sowie den seit 2021 durchgeführten Arbeiten zur Cyber-Einflusskriegsführung bieten wir einen neuen Ansatz zur Automatisierung des Managements von Vorfällen im Informationsbereich an, während spezifische Implementierungskosten und Zeitrahmen begrenzt werden.

Durch die Kombination der Expertise von Airbus in den Bereichen Cybersicherheit und Verteidigung können wir integrierte, durchgängige technische und operative Fähigkeiten bereitstellen, die der Militärdoktrin von 2021 zur Cyber-Informationskriegsführung entsprechen.

## EINE KOMPLETTE, MODULARE LÖSUNG

- Umfassende Datenerfassung mithilfe unserer Partner
- Massenverarbeitung von Daten, KI-Fähigkeiten
- Tiefgehende Analyse und Erkennung von Verhaltensmustern
- Auswertung über souveräne Incident-Response-Tools
- Training mit realistischen Tools zur Animation der Informationsumgebung

Unsere Fähigkeiten im Bereich der Cyber-Informationskriegsführung basieren auf unserer internen Expertise und souveränen Komponenten sowie auf einem vollständigen Ökosystem französischer und europäischer Partner, das wir verwalten.

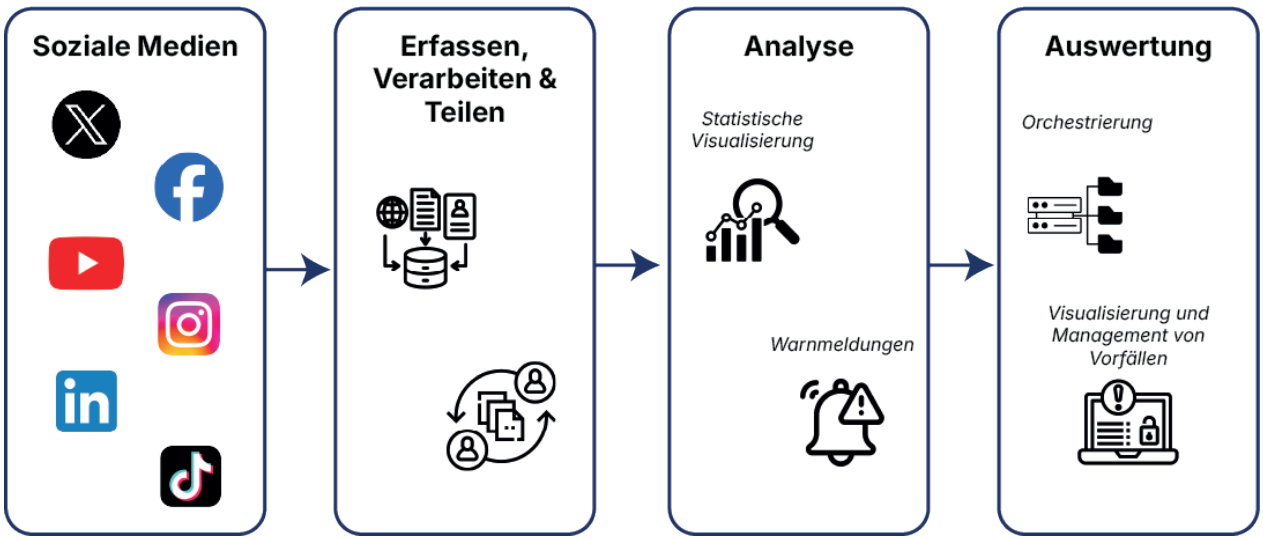
Unsere Lösungen können schrittweise eingeführt werden, um den Aufbau von Kompetenzen in diesem Bereich zu unterstützen.

## Automatisierte Erkennungskette

Wir integrieren alle Komponenten der Wertschöpfungskette der Cyber-Informationskriegsführung:

- Erfassung und Untersuchung von Inhalten in sozialen Netzwerken
- Sammlung und Berichterstattung über Trends
- Analyse der Zuverlässigkeit von Informationsquellen
- Untersuchung von Konten und Profilen, Charakterisierung des digitalen Fußabdrucks von Personen
- Multi-Source-Intelligence-Analyse
- Tools zur Bedrohungserkennung, Orchestrierung, Vorfallbewältigung und Beseitigung, maßgeschneidert für die Bedürfnisse der Computer Network Defence (CND)

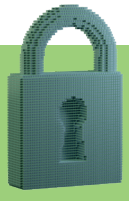
Dieser Ansatz ermöglicht es uns, einen Werkzeugkasten bereitzustellen, der leicht erweiterbar ist und stets dem neuesten Stand der Technik entspricht.




## Souveräne Lösungen

Wir bieten operative Fähigkeiten, die Datenerfassung, Analyse und Auswertung abdecken.

Am Ende der Kette kann ein Lagebericht an das Cyber-Kommando- und Kontrollzentrum weitergegeben werden.



# Training im Informationskrisenmanagement

Mit dem Aufstieg sozialer Medien und der rasanten Entwicklung künstlicher Intelligenz wird die Informationsumgebung zunehmend Ziel von Desinformationskampagnen und Datenschutzverletzungen. Menschliche Analyse reicht nicht mehr aus, um der massiven Verbreitung manipulierter Informationen entgegenzuwirken, insbesondere durch Technologien wie „Deepfakes".

Angesichts dieser neuen Bedrohungen ist ein Informationskrisenmanagement unerlässlich. Der Einsatz technologischer Tools, die in der Lage sind, diese hybriden Bedrohungen schnell zu erkennen, ist entscheidend – kombiniert mit menschlicher Analyse, um sowohl im zivilen als auch im militärischen Bereich eine wirksame Gegenreaktion zu ermöglichen.

## COGNITIO Trainingsmodul

Wir bieten ein Trainingsmodul für das Informationskrisenmanagement an, das eine Simulation der Informationsumgebung beinhaltet und darauf ausgelegt ist, das Training zur Erkennung und Reaktion auf digitale Einflusskampagnen zu erleichtern.

Dieses Modul verfolgt drei Hauptziele:

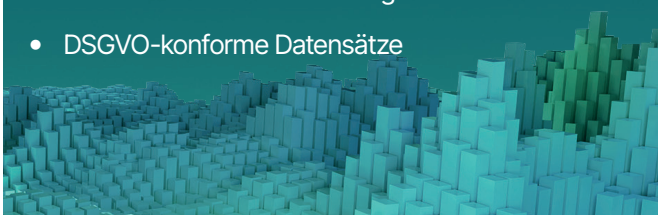
- **Prävention:** Sensibilisierung der Mitarbeiter für Desinformationskampagnen, frühzeitige Erkennung hybrider Bedrohungen und Begrenzung ihres Auftretens
- **Krisenmanagement:** Schnelle Erkennung und Bewertung von Bedrohungen, Eskalation von Sicherheitswarnungen und Echtzeit-Umsetzung von Gegenmaßnahmen
- **Evaluation :** Bewertung der Wirksamkeit des Krisenmanagements und Identifizierung potenzieller Verbesserungsbereiche, sowohl hinsichtlich des Trainings als auch der organisatorischen Aspekte des Krisenmanagementsystems

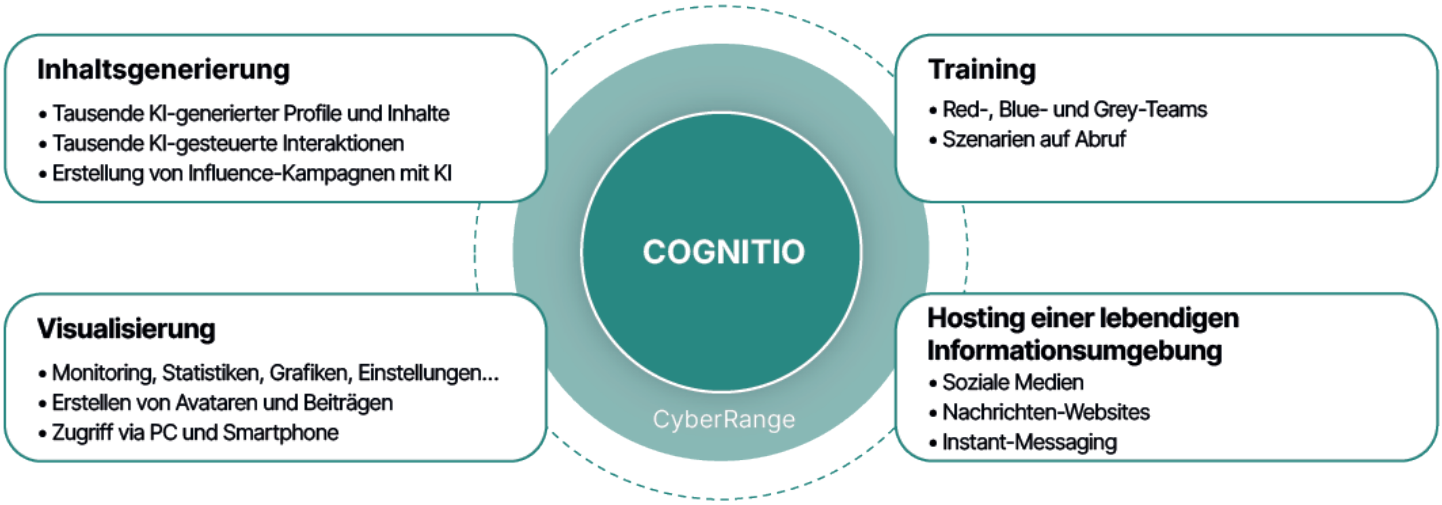
## Immersives Training

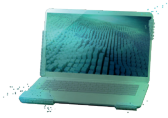
Das Cognitio-Modul, das direkt in unsere CyberRange-Lösung integriert ist, wurde entwickelt, um Cybersecurity-Analysten bei der Antizipation, Erkennung und Abwehr von Desinformationskampagnen zu unterstützen.

**Cognitio bietet:**

- Eine immersive Umgebung
- Automatisierte Inhaltsgenerierung mittels generativer KI
- KI-gesteuerte Generierung von Leben
- Szenarien auf Abruf mit wenigen Klicks
- DSGVO-konforme Datensätze





*Mehrere Übungen des französischen Verteidigungsministeriums haben im Rahmen einer Dienstleistungserbringung von COGNITIO profitiert. Alle Rückmeldungen waren positiv.*

# EUropäischer Cyber- und INFormationskriegsführung- Toolbox

Airbus Defence and Space koordiniert das EUCINF-Projekt*, das darauf abzielt, die Herausforderungen der kognitiven Kriegsführung mithilfe modernster KI-basierter Technologien zu bewältigen.

Ziel ist es, Desinformation sofort nach ihrer Veröffentlichung zu erkennen und ihr entgegenzuwirken, wodurch die europäischen Fähigkeiten im Bereich der Informationskriegsführung durch die Entwicklung einer gemeinsamen Bibliothek erheblich verbessert werden, die innovative Produkte und Software in diesem Bereich zusammenführt.

Airbus koordiniert dieses Projekt der Europäischen Kommission mit Unterstützung von acht EU-Mitgliedstaaten und dem CIDCC (Cyber and Information Domain Coordination Centre). Das Konsortium vereint Experten aus 12 Ländern und 22 Partnern im Bereich Informationskriegsführung, KI und Cybersicherheit, darunter große Unternehmen, KMU und Universitäten.

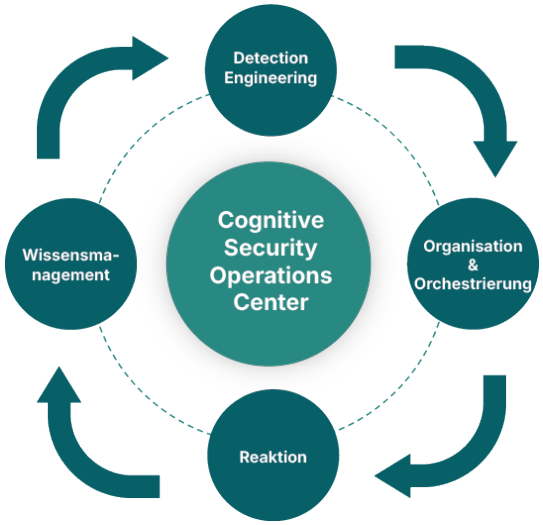
Dieser einzigartige Ansatz ermöglichte die Bereitstellung einer experimentellen Plattform und konfigurierbarer Anwendungen, die als Use-Cases für die zivile und militärische Informationskriegsführung dienen.


## Realistische Szenarien entwickeln

- Das EUCINF-Projekt umfasst drei operationelle Szenarien.
- Spezifische Fallstudien werden durchgeführt, um den Bedürfnissen der teilnehmenden Verteidigungsministerien und bestimmter ziviler Akteure gerecht zu werden, unter Einhaltung der geltenden Vorschriften und gesellschaftlichen Erwartungen.
- Lösungen, die von einem oder mehreren Partnern entwickelt wurden, werden eingesetzt, um Bedrohungen schnell zu erkennen, zu bewerten und zu adressieren, insbesondere durch die Automatisierung von Prozessen mittels künstlicher Intelligenz und Plattform-Interoperabilität.

EUCINF

European Commission




EUCINF demonstriert seine Relevanz und Wirksamkeit auf strategischer, operativer und taktischer Ebene im Kontext der Informationskriegsführung kombiniert mit Computer Network Defence sowohl im zivilen als auch im militärischen Bereich.

*Das EUCINF-Projekt wird von der Europäischen Union unter der Fördervereinbarung Nr. 101121418 kofinanziert. Die geäußerten Ansichten und Meinungen stammen jedoch ausschließlich vom Autor/von den Autoren und spiegeln nicht unbedingt die der Europäischen Union oder der Europäischen Kommission wider. Weder die Europäische Union noch die bewilligende Behörde können dafür verantwortlich gemacht werden.*

**Airbus Defence and Space**
Frankreich, Deutschland, Vereinigtes Königreich, Spanien



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

AIRBUS