TD3 - ANALYSE DES MENACES INFORMATIONNELLES

Analyse de campagnes de désinformation

ESILV | Social listening & Cognitive warfare | Durée : 3 heures

CONTEXTE OPÉRATIONNEL

Vous intégrez une cellule d'Informational Threat Intelligence (ITI). Une campagne de désinformation coordonnée a été détectée autour d'un projet d'infrastructure critique : un parc éolien offshore en Loire-Atlantique.

Votre mission : analyser les indicateurs de compromission (IOC), identifier les patterns de coordination, et produire un rapport d'intelligence actionnable selon les standards OTAN.

Objectifs pédagogiques

Au terme de ce TD, vous serez capables de :

1. **Ingérer et normaliser** des données multi-sources (OSINT social media)
2. **Détecter les contenus synthétiques** (deepfakes textuels et visuels)
3. **Identifier les comportements coordonnés inauthentiques** (CIB)
4. **Cartographier les réseaux d'influence** avec des outils de graph analysis
5. **Coter le renseignement** selon la norme OTAN
6. **Produire un rapport** structuré avec taxonomie DISARM

DONNÉES À DISPOSITION

Dataset	Type	Volume	Usage principal
`tweets_dataset.csv`	CSV	96 tweets	Analyse temporelle, détection CIB
`facebook_posts.json`	JSON	40 posts	Analyse narrative multi-plateforme
`metadata_comptes.json`	JSON	50 profils	Profilage comportemental
`relations_network.csv`	CSV	211 interactions	Graph analysis (GEPHI)
`textes_analyse_sentiment.txt`	TXT	55 textes	Analyse NPL
`dossier images/`	Images	~30 fichiers	Détection deepfakes visuels (PeREN)
`articles_web.txt`	TXT	4 articles	Analyse des narratifs

Volume total : ~500 entités à analyser | **Période** : 7 jours | **Langues** : Français

---

STACK TECHNIQUE

Frameworks & Outils

- **D3lta** (VIGINUM) : Détection de duplication de contenu par embeddings FAISS
- **PeREN** : Métadétecteur d'images générées par IA (Pôle d'Expertise Régulation Numérique)
- **BERTopic** : Topic modeling pour analyse narrative
- **GEPHI** : Visualisation et analyse de réseaux sociaux
- **DISARM Framework** : Taxonomie des techniques de désinformation (MITRE-style)

CADRE CONCEPTUEL

Taxonomie des manipulations informationnelles

Type	Définition	Intentionnalité	Exemple

Type	Définition	Intentionnalité	Exemple
Désinformation	Information fausse créée et diffusée intentionnellement	✓ Intentionnelle	Faux document "confidentiel" préfecture
Mésinformation	Information fausse partagée sans intention de nuire	✗ Non intentionnelle	Partage d'infox par erreur de bonne foi
Malinformation	Information vraie utilisée pour nuire (doxing, leaks)	✓ Intentionnelle	Publication données personnelles

> **Focus du TD** : Nous analysons ici de la **désinformation** (adversarial information operations).

Coordinated Inauthentic Behavior (CIB)

Définition opérationnelle : Utilisation de multiples assets (comptes réels, faux, bots) agissant de manière synchronisée pour amplifier artificiellement un narratif, en violation des CGU des plateformes.

Indicateurs techniques :

- **Temporal clustering** : création de comptes dans une fenêtre temporelle réduite (<30 jours)
- **Behavioral synchronization** : publication de contenus similaires à des timestamps proches (<15 min)
- **Amplification circulaire** : retweets/shares mutuels formant des clusters denses (densité >0.7)
- **Asset generation** : utilisation de profils synthétiques (GAN-generated faces, bios LLM)

Deepfakes : typologie

Modalité	Techniques	Outils courrants	Détection
Visuel	GAN (StyleGAN2/3), Diffusion (SD, MJ)	Midjourney, DALL-E, Stable Diffusion	PeREN
Textuel	LLM (GPT-3.5+, Llama, Mistral)	ChatGPT, Claude, open-source LLMs	Perplexité, détecteurs GPTZero/Originality.ai

EXERCICE 1 : Ingestion et preprocessing (20 min)

Objectif

Dans une investigation de menace informationnelle, les adversaires opèrent sur **plusieurs vecteurs simultanément** (Twitter, Facebook, sites web, forums). Analyser une seule source = vision tunnel. Vous devez construire un **dataset unifié multi-sources** pour détecter les patterns multi-platforme.

Cas d'usage réel : Opération Secondary Infektion

En 2019, des chercheurs de l'Atlantic Council ont détecté une campagne russe sur **6 plateformes** (Facebook, Twitter, Reddit, Medium, Change.org, forums locaux) diffusant les mêmes documents falsifiés en 7 langues. La détection n'a été possible qu'en **corrélant les timestamps et contenus multi-plateforme**.

Source : DFRLab Report - Secondary Infektion

Tâches

1.1 - Charger les données brutes

```
import pandas as pd
import json
from datetime import datetime

# Tweets
tweets_df = pd.read_csv('donnees/tweets_dataset.csv')
tweets_df['date'] = pd.to_datetime(tweets_df['date'])
tweets_df['platform'] = 'twitter'
tweets_df['content_type'] = 'tweet'

# Facebook posts
with open('donnees/facebook_posts.json', 'r', encoding='utf-8') as f:
    fb_data = json.load(f)

fb_df = pd.DataFrame(fb_data)
fb_df['post_date'] = pd.to_datetime(fb_df['post_date'])
fb_df['platform'] = 'facebook'
fb_df['content_type'] = 'post'

# Articles web
with open('donnees/articles_web.txt', 'r', encoding='utf-8') as f:
    articles_raw = f.read()

# Parser les articles (format à adapter selon structure réelle)
```

1.2 - Normaliser le schéma de données

Objectif : créer un schéma pivot unique pour l'analyse multi-plateforme.

```
# Schéma cible unifié
schema = {
    'id': 'unique_id',
    'platform': 'twitter|facebook|web',
    'author': 'username|page_name',
    'content': 'text',
    'timestamp': 'datetime',
    'engagement': 'likes + shares + comments',
    'content_type': 'tweet|post|article'
}

# Normalisation tweets
tweets_norm = tweets_df.rename(columns={
    'username': 'author',
    'text': 'content',
    'date': 'timestamp'
})
```

```
tweets_norm['engagement'] = tweets_norm['likes'] + tweets_norm['retweets']
tweets_norm['id'] = 'tw_' + tweets_norm.index.astype(str)

# Normalisation Facebook
fb_norm = fb_df.rename(columns={
    'page_name': 'author',
    'content': 'content',
    'post_date': 'timestamp'
})
fb_norm['engagement'] = fb_norm['likes'] + fb_norm['shares'] + fb_norm['comments']
fb_norm['id'] = 'fb_' + fb_norm.index.astype(str)

# Merge final
dataset_unifie = pd.concat([
    tweets_norm[['id', 'platform', 'author', 'content', 'timestamp', 'engagement',
'content_type']],
    fb_norm[['id', 'platform', 'author', 'content', 'timestamp', 'engagement',
'content_type']]
], ignore_index=True)

# Export
dataset_unifie.to_csv('dataset_unifie.csv', index=False)
print(f"Dataset unifié créé : {len(dataset_unifie)} entrées")
```

1.3 - Analyse exploratoire temporelle

```
import matplotlib.pyplot as plt

# Distribution temporelle par plateforme
dataset_unifie['date'] = dataset_unifie['timestamp'].dt.date

platform_timeline = dataset_unifie.groupby(['date',
'platform']).size().unstack(fill_value=0)

plt.figure(figsize=(12,6))
platform_timeline.plot(kind='line', marker='o')
plt.title('Timeline d\'activité multi-plateforme')
plt.xlabel('Date')
plt.ylabel('Nombre de publications')
plt.legend(title='Platform')
plt.grid(True, alpha=0.3)
plt.savefig('timeline_crossplatform.png', dpi=300)
```

Questions d'analyse

1. **Quelle plateforme présente le volume d'activité le plus important ?**
2. **Identifiez-vous des pics d'activité synchronisés entre plateformes ?** (indicateur de campagne coordonnée)
3. **Quel est le ratio engagement/publication moyen par plateforme ?**

Livrables attendus

`preprocess_data.py` - Script d'ingestion `dataset_unifie.csv` - Dataset normalisé
`timeline_crossplatform.png` - Visualisation temporelle

EXERCICE 2A : Analyse sémantique avec d3lta

Contexte opérationnel : Copypasta & Astroturfing

Astroturfing : Technique consistant à créer une fausse impression de mouvement grassroots en dupliquant le même message via de multiples comptes.

Cas réel : En 2021, Facebook a supprimé un réseau de 150 comptes qui postaient **le même contenu mot pour mot** en changeant juste 2-3 mots (Meta Q2 2021 Adversarial Threat Report).

D3lta : Fonctionnement

D3lta (développé par VIGINUM - service français de vigilance contre les ingérences numériques) utilise des **embeddings sémantiques** pour détecter :

- Duplications exactes (copypasta)
- Reformulations syntaxiques (même sens, mots différents)
- Traductions cross-langues

Architecture :

1. Encodage des textes via sentence-transformers (`paraphrase-multilingual-mpnet-base-v2`)
2. Indexation FAISS pour recherche de similarité rapide
3. Clustering hiérarchique pour détecter les groupes de contenus dupliqués

Installation et configuration

Analyse des patterns de coordination

Extraire les comptes participant à plusieurs clusters

Identifier les comptes multi-clusters (coordination suspecté)

Questions d'analyse

1. **Quel est le plus grand cluster de duplication détecté ?** (nombre de messages)
2. **Identifiez les 5 comptes les plus actifs dans la duplication de contenu**
3. **Y a-t-il des patterns temporels dans les duplications ?** (tous publiés le même jour ?)
4. **Le contenu dupliqué porte-t-il sur des narratifs spécifiques ?** (environnement, économie, santé ?)

Livrable

☑ `clusters_coordination.md` - Rapport des clusters détectés avec comptes impliqués

EXERCICE 2B : Topic Modeling avec BERTopic (20 min)

Objectif

Identifier les **narratifs structurants** d'une campagne de désinformation. Un narratif = récit cohérent qui oriente l'interprétation d'un événement.

Exemple : Narratif "Complot élites mondialistes" → Tous les événements sont réinterprétés comme des actions d'une élite cachée.

BERTopic : Principes

BERTopic utilise des embeddings transformers + UMAP + HDBSCAN pour identifier automatiquement les topics sans supervision.

Avantages vs LDA classique :

- Comprend le contexte sémantique (pas juste des mots-clés)
- Fonctionne bien sur de petits corpus (<1000 documents)
- Génère des labels de topics interprétables

Tâches

2C.1 - Préparation et entraînement du modèle

Charger les contenus

Configuration BERTopic

Entraîner le modèle

Sauvegarder le modèle

Obtenir les topics

Visualiser les topics principaux

Visualisation interactive

Questions d'analyse

1. **Combien de topics distincts ont été identifiés par BERTopic ?**
2. **Quel topic est le plus représenté dans le corpus ?**
3. **Y a-t-il un topic clairement associé à la désinformation ?**
4. **Quels mots-clés caractérisent ce topic ?**

Livrable

`bertopic_results.md` - Analyse des topics avec annotations et prévalence

EXERCICE 3 : Analyse de réseau avec GEPHI (30 min)

Objectif

Visualiser les **structures de coordination** dans les réseaux sociaux. Les campagnes CIB créent des patterns de graphe distinctifs détectables par analyse topologique.

Différences structurelles :

Réseau organique	Réseau coordonné (CIB)
Structure dispersée, hubs naturels	Clusters ultra-denses (cliques)
Croissance progressive	Apparition soudaine de comptes
Interactions spontanées	Amplification circulaire synchronisée
Modularité modérée (0.3-0.5)	Modularité élevée (>0.6)

Métriques clés de graph analysis

Métrique	Définition	Interprétation
Degré (Degree)	Nombre de connexions d'un nœud	Influence/centralité du compte
Betweenness centrality	Nombre de chemins passant par un nœud	Compte "pont" entre clusters, rôle de diffusion
Modularité (Modularity)	Qualité de la division en communautés	>0.6 = excellente séparation, suspect si clusters trop denses
Densité (Density)	% de liens réels / liens possibles	>0.7 dans un cluster = coordination suspecte

Procédure GEPHI

Étape 1 : Import des données

```
1. Ouvrir GEPHI
2. Fichier → Importer feuille de calcul
3. Sélectionner : donnees/relations_network.csv
4. Type : Table de lien
```

```
5. Configuration :
   - Source : colonne "source"
   - Target : colonne "target"
   - Sélectionner TimeStampStringMap pour timestamp
   - Type de graphe : Directed (orienté)
6. Importer dans nouveau projet
```

Étape 2 : Calcul des statistiques

```
Panneau Statistiques (droite) → Exécuter :

1. Diamètre du réseau
   → Mesure la distance maximale entre deux nœuds

2. Degré moyen
   → Nombre moyen de connexions par compte

3. Modularité (algorithme Louvain)
   → Détecte automatiquement les communautés
   → Résultat attendu : ~0.5
   → Nombre de communautés : ~3-5

4. Centralité d'intermédiarité (Betweenness)
   → Identifie les comptes "ponts" entre clusters
```

Étape 3 : Spatialisation (Layout)

```
Panneau Disposition → ForceAtlas2 :

Paramètres recommandés :
- Scaling : 10
- Gravity : 1.0
- ✓ Prevent Overlap (éviter chevauchement nœuds)
- ✓ LinLog mode (optionnel, pour mieux séparer les clusters)

Lancer → Laisser stabiliser 30-60s → Arrêter
```

Étape 4 : Visualisation

```
Panneau Apparence :

1. Couleur par Communauté :
   - Nodes → Partition → Betweenness Centrality
   → Chaque communauté = couleur différente

2. Taille par Degré :
   - Nodes → Ranking → Degree
```

```
   - Min: 10, Max: 50
   → Comptes influents = gros nœuds

3. Labels :
   - Activer (icône T en bas)
   - Proportionnels au degré
   - Afficher si degré > 5 (pour lisibilité)
```

Étape 5 : Export

```
Fichier → Exporter → PNG
Résolution : 2000×2000
Transparence : Activé

Fichier → Enregistrer le projet → reseau.gephi
```

Analyse des résultats

4.1 - Identifier les clusters suspects

Créez ce tableau en analysant le graphe GEPHI :

Communauté	Couleur	Nb Nœuds	Densité	Type	Comptes centraux
id	Rouge	N	0.X	**SUSPECT**	XXXX , XXXX, XXXX

Critères de suspicion :

- Densité >0.65 (interactions trop fréquentes)
- Noms de comptes similaires (même convention de nommage)
- Création temporelle groupée (vérifier dans metadata_comptes.json)

4.2 - Identifier les influenceurs et diffuseurs

```
Trier les nœuds par :
- Degré (top 10) → Comptes les plus connectés
- Betweenness (top 10) → Comptes "ponts" entre communautés
```

Questions d'analyse

1. **Structure du réseau** :
    - Nombre de communautés détectées ?
    - Score de modularité global ?
    - Présence de clusters ultra-denses (densité >0.7) ?
2. **Comptes centraux** :

- Top 5 par degré ?
- Top 5 par betweenness ?
- Ces comptes appartiennent-ils aux clusters suspects ?

3. **Patterns de coordination** :

- Interactions majoritairement intra-cluster ou inter-cluster ?
- Présence d'amplification circulaire (A retweet B, B retweet C, C retweet A) ?
- Synchronisation temporelle des interactions ?

Livrable

`reseau.png` - Export du graphe GEPHI coloré

EXERCICE 4 : Cotation du renseignement - Admiralty Code (20 min)

Contexte : Intelligence Assessment

Dans le renseignement militaire et gouvernemental, chaque information collectée doit être **cotée** selon deux axes indépendants :

Admiralty Code :

- **Axe 1** : Fiabilité de la SOURCE (A à F)
- **Axe 2** : Crédibilité de l'INFORMATION (1 à 6)

Principe clé : Une source fiable (A) peut transmettre une information fausse (5), et inversement, une source douteuse (E) peut transmettre une information vraie (1). Les deux axes sont **indépendants**.

Grille de cotation

FIABILITÉ DE LA SOURCE :

Code	Libellé	Définition	Exemple
A	Fiable	Source éprouvée, historique de véracité	Compte officiel préfecture, chercheur CNRS
B	Généralement fiable	Source connue, occasionnellement inexacte	Journaliste reconnu, média local établi
C	Assez fiable	Source correcte dans le passé	Compte citoyen engagé, blog spécialisé
D	Généralement non fiable	Source suspecte, erreurs fréquentes	Compte récent, profil anonyme
E	Non fiable	Source déjà prise en flagrant délit de désinformation	Compte diffusant des fausses infos avérées
F	Fiabilité impossible à évaluer	Première interaction, pas d'historique	Nouveau compte, source anonyme sans historique

CRÉDIBILITÉ DE L'INFORMATION :

Code	Libellé	Définition	Critères de vérification
1	Confirmée	Information vérifiée par sources indépendantes	Recoupement 3+ sources fiables, preuves tangibles
2	Probablement vraie	Logique, cohérente avec informations confirmées	Cohérence narrative, absence de contradictions
3	Possiblement vraie	Compatible avec connaissances, non vérifiée	Plausible mais non recoupée
4	Douteuse	Incohérente, contradictoire	Éléments suspects, contradictions internes
5	Improbable	En contradiction avec informations confirmées	Contredit des faits établis
6	Véracité impossible à évaluer	Informations insuffisantes	Impossible à vérifier avec sources disponibles

Exemples de cotation :

- **A1** : Communiqué de presse préfecture sur dates d'enquête publique (source officielle + vérifiable)
- **B2** : Article Ouest-France citant sources préfecture (média établi + cohérent)
- **D5** : Tweet compte récent affirmant "87% dauphins impactés" sans source (compte suspect + contredit études)
- **E5** : Post Facebook "rapport confidentiel" avec document falsifié (compte déjà flagué + faux avéré)
- **F6** : Témoignage anonyme invérifiable (source inconnue + impossible à vérifier)

Tâches

5.1 - Extraire 10 affirmations à coter

Sélectionnez 10 affirmations factuelles du dataset (mix sources fiables/suspectes) :

```
# Exemples d'affirmations à extraire et coter
affirmations = [
    {
        'id': 'AFF_001',
        'source': 'PrefectureLoire',
        'date': '2024-01-16',
        'texte': "L'enquête publique se déroule du 20 janvier au 15 février. Tous
les documents sont consultables en mairie.",
        'type_source': 'officiel',
        'source_historique': 'compte_verifie'
    },
    {
        'id': 'AFF_002',
        'source': 'AlerteVerite2024',
        'date': '2024-01-15',
```

```
        'texte': "Un document confidentiel révèle que 87% des dauphins seront
impactés. Les autorités cachent la vérité !",
        'type_source': 'citoyen',
        'source_historique': 'compte_recent_suspect'
    },
    # ... 8 autres affirmations
]
```

5.2 - Coter chaque affirmation

Pour chaque affirmation, documenter le raisonnement :

```
### AFFIRMATION 001

**Texte** : "L'enquête publique se déroule du 20 janvier au 15 février. Tous les
documents sont consultables en mairie."

**Source** : PrefectureLoire (compte officiel vérifié)

**Cotation** : **A2**

**Justification** :
- **Fiabilité source (A)** :
  - Compte officiel gouvernemental vérifié
  - Historique de communications officielles fiables
  - Mandat pour diffuser ce type d'information

- **Crédibilité information (2)** :
  - Information procédurale vérifiable
  - Cohérente avec le cadre légal des enquêtes publiques
  - Dates et modalités précises
  - Cotation "2" et non "1" car non encore recoupée par source indépendante au
moment de l'analyse

**Vérification possible** : Consulter site web préfecture, contacter mairies
concernées
```

5.3 - Créer le tableau de synthèse

ID	Source	Cotation	Texte (extrait)	Justification synthétique
...	...	...	...	...

Questions d'analyse

1. **Distribution des cotations** :
   - Combien d'affirmations cotées A ou B (sources fiables) ?
   - Combien cotées 4 ou 5 (informations improbables/douteuses) ?

2. **Patterns de désinformation** :
    - Les sources D/E produisent-elles majoritairement de l'information 4/5 ?
    - Y a-t-il des cas de sources A avec information 5 ? (erreur exceptionnelle ou compromission ?)
3. **Affirmations critiques** :
    - Quelle affirmation est la plus dangereuse ? (combinaison crédibilité source + impact narratif)
    - Quelles affirmations nécessitent une fact-check en priorité ?

Livrable

☑ `cotation_amiraute.md` - Tableau des 10 affirmations cotées avec justifications

---

EXERCICE 6 : Note de Renseignement (40 min)

Format : Note d'Intelligence selon standard DISARM

Vous allez produire une **Note de Renseignement** synthétisant votre analyse, destinée à un RSSI ou un décideur politique. La note doit être :

- **Concise** : 3 pages maximum
- **Structurée** : Template standard avec sections obligatoires
- **Actionable** : Recommandations opérationnelles concrètes
- **Sourcée** : Toutes affirmations appuyées sur l'analyse

Template de Note de Renseignement

```
# NOTE DE RENSEIGNEMENT
## Analyse de Campagne de Désinformation - Projet Éolien Offshore Loire-Atlantique

**Mention de protection** : NON PROTEGE
**Référence** : NP-2025-001-EOLIEN-LOIRE
**Date** : [Date de production]
**Analyste** : [Votre nom]
**Destinataire** : Direction Cybersécurité & Sûreté

---

## RÉSUMÉ EXÉCUTIF (Executive Summary)

[3-5 lignes maximum - Répondre à : Quelle menace ? Quelle ampleur ? Quel impact ?]


---

## SYNTHÈSE DES INDICATEURS

### Données collectées
- **Période d'observation** : 15-20 janvier 2024 (7 jours)
- **Plateformes** : Twitter, Facebook, sites web
```

```
- **Volume** : 96 tweets, 40 posts FB, 55 textes, ~30 images
- **Portée estimée** : [Calculer : somme des followers des comptes suspects]

### Indicateurs de Coordinated Inauthentic Behavior (CIB)

| Indicateur | Valeur | Seuil suspect | Verdict |
|-----------|--------|---------------|---------|
| Clusters D3lta (duplication) | [X] clusters | >2 | ⚠ [ALERTE/OK] |
| Comptes créés <30j | [X]% | >40% | ⚠ [ALERTE/OK] |
| Densité réseau cluster max | 0.[XX] | >0.65 | ⚠ [ALERTE/OK] |
| Images IA-générées (PeREN >0.7) | [X]/30 | >10% | ⚠ [ALERTE/OK] |
| Textes signature LLM | [X]/55 | >20% | ⚠ [ALERTE/OK] |

**Conclusion** : [Présence confirmée / Présence probable / Absence] de campagne
CIB coordonnée.

---

## ANALYSE DES ACTEURS

### Clusters de coordination identifiés

**CLUSTER 1 - "XXXXXX"** (Densité réseau : 0.XX)
- **Comptes principaux & principaux relais** :
- **Création** :
- **Comportement** :
- **Narratif** :
- **Cotation moyenne** :


### Comptes à haute influence (Top 5 betweenness centrality)

1. **[Compte_1]** - [Rôle] - Degré : [X], Betweenness : [Y]
2. [...]

---

## ANALYSE DES NARRATIFS

### Topic Modeling (BERTopic)

**Narratifs identifiés** :

| Topic ID | Label | Type | Mots-clés principaux |
|----------|-------|------------|------|--------------------|


**Narratif dominant de désinformation** : [Décrire le topic principal suspect]

### Techniques DISARM identifiées

Mapper les techniques observées selon le framework DISARM :

| Technique DISARM | Description | Preuves observées |
```

```
|-----------------|-------------|------------------|


**Référence** : [DISARM Framework]
(https://github.com/DISARMFoundation/DISARMframeworks)

---

## IMPACT ET RISQUES

### Risques d'impact

- **Comptes exposés** : [Somme followers comptes principaux]
- **Viralité** : [Ratio shares/posts]
- **Impressions estimées** : [Calculer : somme engagement × facteur viralité sur
le ou les narratifs à risque]

### Risques identifiés

## PLAN D'ACTIONS
---

## RESSOURCES COMPLÉMENTAIRES

### Documentation officielle

- **DISARM Framework** : https://disarmfoundation.github.io/disarm-navigator/
- **D3lta (VIGINUM)** : https://github.com/VIGINUM-FR/D3lta
- **GEPHI Tutorials** : https://gephi.org/users/
- **BERTopic Docs** : https://maartengr.github.io/BERTopic/

### Rapports de référence

- VIGINUM Rapports publics : https://www.sgdsn.gouv.fr/publications?
field_type_target_id%5B182%5D=182
- DFRLab (Atlantic Council) : https://www.atlanticcouncil.org/programs/digital-
forensic-research-lab/

---

**ESILV - Social listening & cognitive warfare**
*Document pédagogique - Utilisation autorisée dans cadre académique uniquement*

---

![ESILV Logo](Charte%20graphique/logo%20ESILV%20b%26r.webp)
```