

DIMA

Un *framework* pour décrire les
attaques cognitives





De quoi parle-t-on ?

La « **désinformation** » est généralement définie comme la diffusion d'informations délibérément fausses ou trompeuses. On parle alors de « fausses informations » ou de « fake news ».

La « **manipulation de l'information** » est une action délibérée (intention de nuire), clandestine (les victimes sont inconscientes) de diffusion d'information falsifiées, déformées ou forgées.

Une **opération d'influence** (OI) combine diffusion d'information et actions physiques dans le but de **modifier des comportements**.

Attaque cognitive ?

Les campagnes de manipulation de l'information visent à **modifier les perceptions des opinions publiques** sur des situations particulières. (renforcement cognitif)

La guerre cognitive vise à altérer directement les mécanismes de compréhension du monde réel et **de prise de décision** pour déstabiliser ou paralyser un adversaire.

« Une attaque cognitive correspond à l'**utilisation intentionnelle d'un ou plusieurs biais ou heuristiques** dont l'objectif est de provoquer une réaction de la cible. »





Les cerveaux humains, vulnérables aux **biais cognitifs**, sont directement ciblés pour « modifier des comportements ».



Objectif de la matrice : **caractérisation des attaques cognitives**. Comprendre les biais exploités par un attaquant potentiel pour qu'une information provoque un changement de comportement.



Il ne s'agit pas ici de « détecter des fake news, » mais d'évaluer à quel point une information reçue est construite (délibérément) pour exploiter un ou plusieurs biais cognitifs.

Renforcer la défense par la connaissance des vulnérabilités exploitées

Pourquoi DIMA ?

Livre blanc sur les manipulations de l'information

Bertrand Boyer
Anais Meunier
M82_project



Que faut-il modéliser et pourquoi ?

Approche tournée vers l'acteur Comprendre l'attaque

La « kill chain »
pour mieux se
défendre

Modéliser le
schéma de
l'attaque;

Approche « cible » Connaitre les vulnérabilités exploitées

Faire émerger
des vulnérabilités
à protéger.

Faire apparaître
des « signatures »
pour caractériser
un acteur

Pour se défendre, il faut soit « briser l'attaque » soit
la rendre inefficace.

ATT&CK Matrix for Enterprise

layout: flat ▾

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Other
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Albedo	Account Takeover	Abuse of Functionality	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Scripting	Abuse of Configuration	Abuse Elevation	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Adversary-in-the-Middle (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration	Access Token Manipulation	Adversary-in-the-Middle (5)	Credentials from Word Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Adversary-in-the-Middle (3)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Command & Control	Account Takeover	Brute Force (14)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Adversary-in-the-Middle (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Container Initialization	Boot or Logon Autostart Execution	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Clipboard Data	Adversary-in-the-Middle (3)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Client Exploitation	Boot or Logon Initialization	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Cloud Storage	Adversary-in-the-Middle (3)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Communication	Create or Modify System Process (5)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Data from Configuration Repository (2)	Data from Information Repositories (3)	Adversary-in-the-Middle (3)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Native API	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Software Deployment Tools	Taint Shared Content	Data from Local System	Adversary-in-the-Middle (3)
Search Open Websites/ Domains (3)	Trusted Relationship	Trusted Relationship	Scheduled Task/ Job (5)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Process (9)	Container and Resource Discovery	Use Alternate Authentication Material (4)	Data from Network Shared	Adversary-in-the-Middle (3)
	Valid Accounts (4)	Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion			Adversary-in-the-Middle (3)
			Shared Modules	External Remote Services	Event Triggered Execution (16)	Multi-Factor Authentication	Device Driver			Adversary-in-the-Middle (3)
			Software Deployment Tools		Exploitation for Defense Evasion					Adversary-in-the-Middle (3)
			System		Exploitation for Defense Evasion					Adversary-in-the-Middle (3)

Méthodologie

- Approche CTI, LMI : MITRE ATT&CK, DISARM (schéma d'attaque) Kill chain.
- Traitement de l'information par le cerveau
- Découpage en **phase/tactique/technique**
- **4 phases - DIMA :**
 - Déetecter,
 - Donner du sens (informer),
 - Retenir (Mémoriser),
 - Agir.

THE CYBER KILL CHAIN



Source :
<https://cybotsai.com/introduction-mitre-attck/>

01

Detect / Détecter

02

Inform / Informer (donner du sens)

03

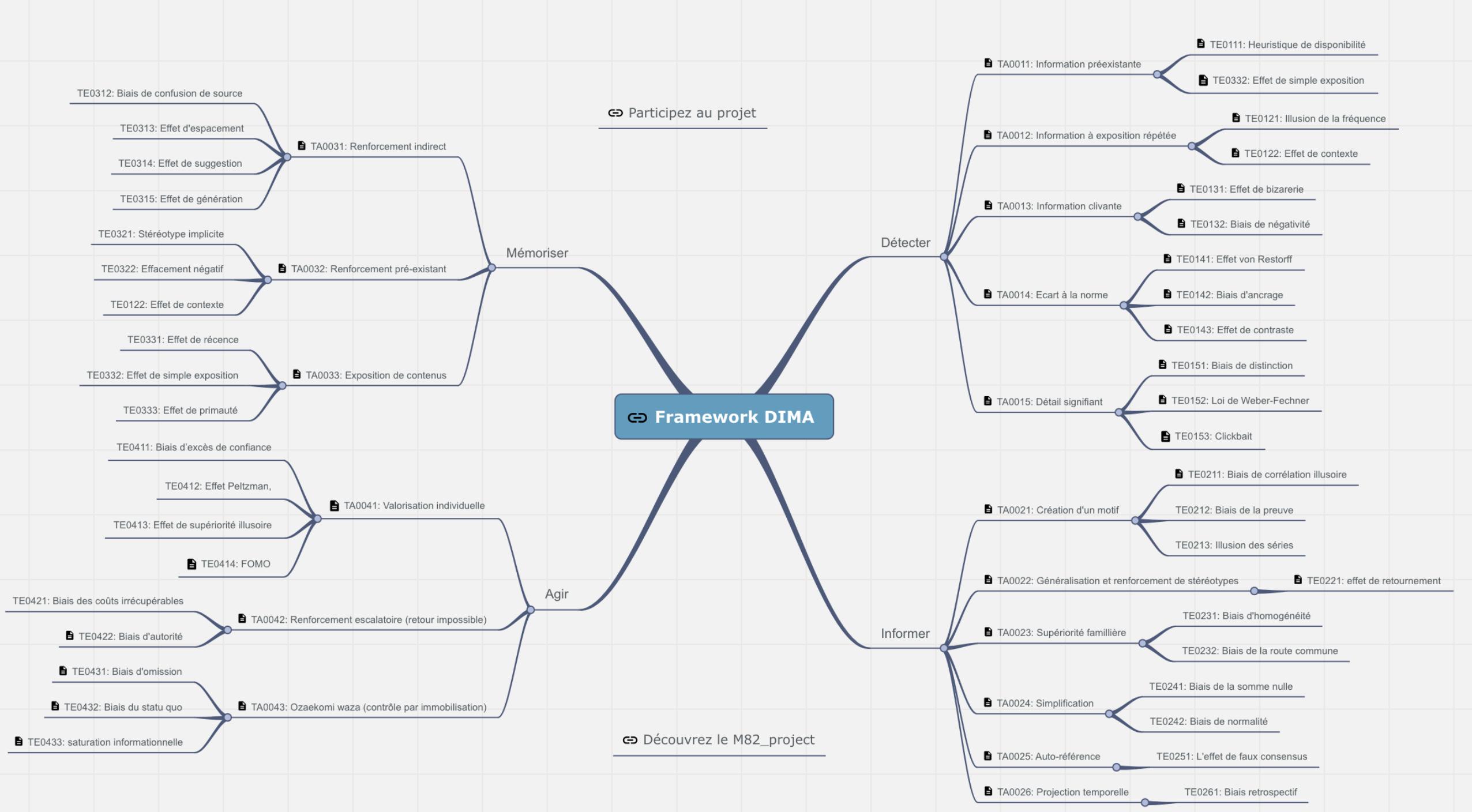
Memorize / Mémoriser (Y/N)

04

Act / Agir



DIMA « Cognitive Kill Chain »



Déte~~c~~ter

POURQUOI CETTE
INFORMATION A-T-ELLE
ATTIRÉ MON ATTENTION
?



Octobre 2023: les « punaises de lit »



Plusieurs médias évoquent le sujet, rumeurs sur les réseaux sociaux. L'information est détectée par l'utilisation de « l'illusion de fréquence ».

Autrement connu sous le nom de phénomène Baader-Meinhof, l'illusion de la fréquence semble être une combinaison de plusieurs biais qui nous amène à pratiquer une forme "d'attention selective".

Ce mécanisme est particulièrement à l'œuvre dans la diffusion des thèses complotistes.

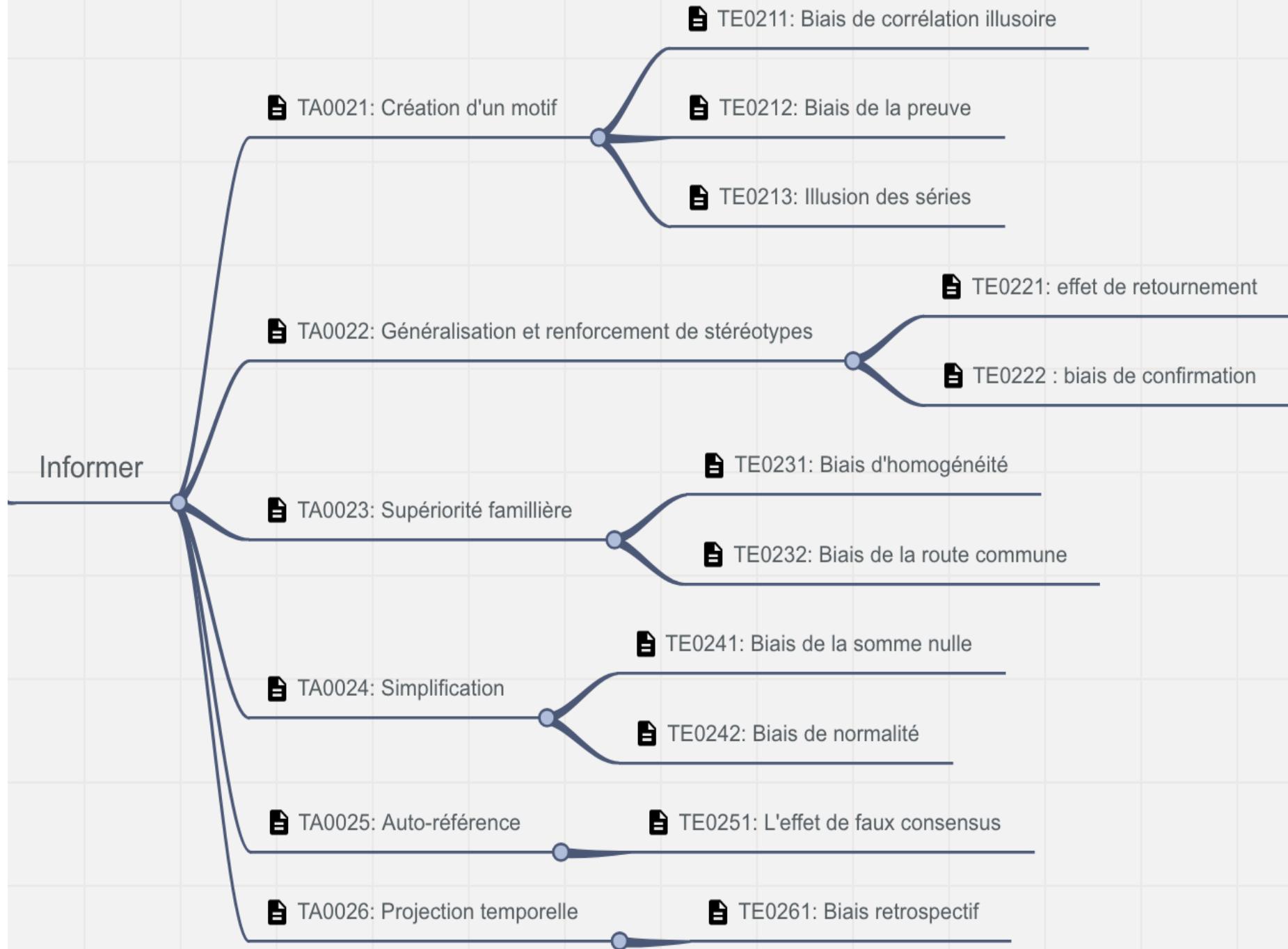
"L'illusion de fréquence consiste, après avoir remarqué une chose une première fois, à avoir tendance à la remarquer plus souvent, ce qui conduit à croire qu'elle se produit plus fréquemment qu'auparavant."

DIMA : TE 0121 « ILLUSION DE FRÉQUENCE »

DISARM : T0042 "Seed Kernel of truth"

Informer

Donner du sens à une information ?



TE 0211: Biais de corrélation illusoire

- Nous donnons du sens à cette information en créant des « corrélations » (i.e – lien entre réfugiés ukrainiens et apparition des parasites)



Société



Les réfugiés ukrainiens ont-ils transporté des punaises de lit à Paris ?

Par E.P

Mis à jour il y a 8 minutes



Le gouvernement a lancé une campagne de lutte contre les punaises de lit à Paris.

Selon les spécialistes, l'épidémie actuelle prend une grande ampleur. La raison en est que des réfugiés ukrainiens affluent à Paris. Les Ukrainiens ramènent des acariens et d'autres parasites sur leurs effets personnels.

Grâce au climat favorable de la France, les insectes se multiplient activement. La plus grande vague de l'épidémie est encore à venir.



Paris Marseille Toulouse

ACCUEIL > PARIS



Paris le 12 avril 2021 — A. G.

ENQUETE

Les punaises de lit se reproduisent à

MIS À JOUR LE 02/10/23 À 08H00

Aude Lorriaux



Des réfugiés ukrainiens de lit et d'autres parasites

France. Les experts pré



COMMENTER



PARTAGER

Mémoriser

- Pourquoi retenir cette information ?

12.biais de confusion de source

TE0313: Effet d'espacement

314: Effet de suggestion

TE0315: Effet de génération

TE0321: Stéréotype implicite

TE0322: Effacement négatif

TE0323: Effet de contexte

TE0331: Effet de récence

0332: Effet de simple exposition

TE0333: Effet de primauté

TA0031: Renforcement indirect

TA0032: Renforcement pré-existant

TA0033: Exposition de contenus

≡

F / Société

•

Les réfugiés ukrainiens
ont-ils transporté des
punaises de lit à Paris ?



TE 0314: effet de suggestion

TE 0321: Stéréotype implicite

- Usage de l'interrogation
- Amplification de stéréotypes



Agir

POUQUOI CETTE INFORMATION PROVOQUE UNE (RE)ACTION DE MA PART ?

TE0411: Biais d'excès de confiance

TE0412: Effet Peltzman,

TE0413: Effet de supériorité illusoire

TE0414: FOMO

TE0421: Biais des coûts irrécupérables

TE0422: Biais d'autorité

TE0431: Biais d'omission

TE0432: Biais du statu quo

TE0433: saturation informationnelle

TA0041: Valorisation individuelle

TA0042: Renforcement escalatoire (retour impossible)

TA0043: Ozaekomi waza (contrôle par immobilisation)

Agir



*TE 0422 : biais
d'autorité*

Les « experts » confirment, ils « prédisent » une épidémie... Il faut donc prendre des mesures.

Les punaises de lit d'Europe de l'Est se reproduisent à Paris

MIS À JOUR LE 02/10/23 À 08H02

Aude Lorriaux 

Des réfugiés ukrainiens ont transporté des punaises de lit et d'autres parasites sur leurs vêtements en France. Les experts prédisent une épidémie.



COMMENTER



PARTAGER



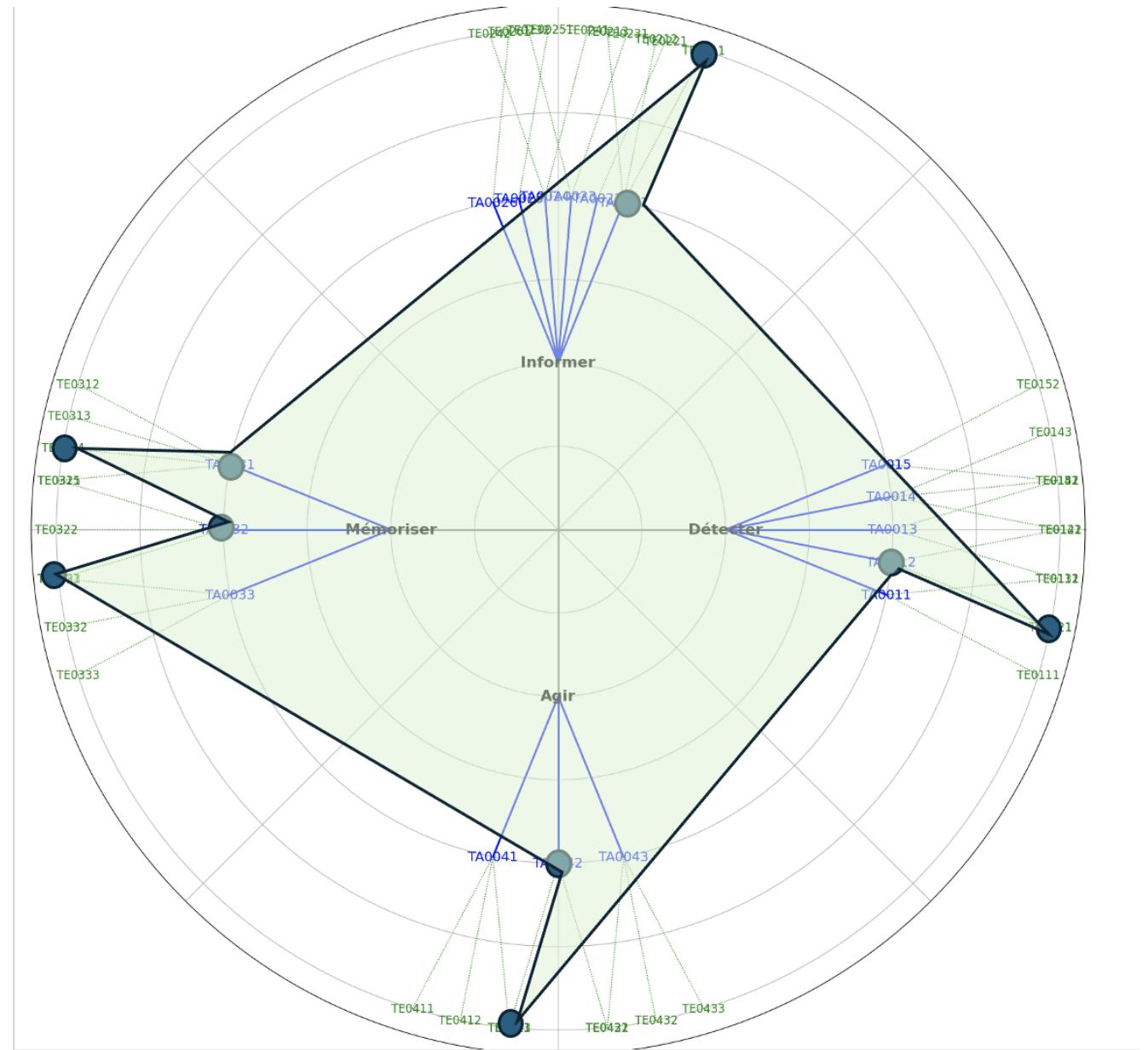
SAUVEGARDER



UNE FAUTE ?

Bilan

- Détecer
 - TA0012: Information à exposition répétée
 - TE0121: Illusion de la fréquence
 - Informer
 - TA0021: Création d'un motif
 - TE0211: biais de corrélation illusoire
 - Mémoriser
 - TA0031: Renforcement indirect
 - TE0314: Effet de suggestion
 - TA0032: Renforcement pré-existant
 - TE0321: Stéréotype implicite
 - Agir
 - TA0042: Renforcement escalatoire
 - TE0422: biais d'autorité

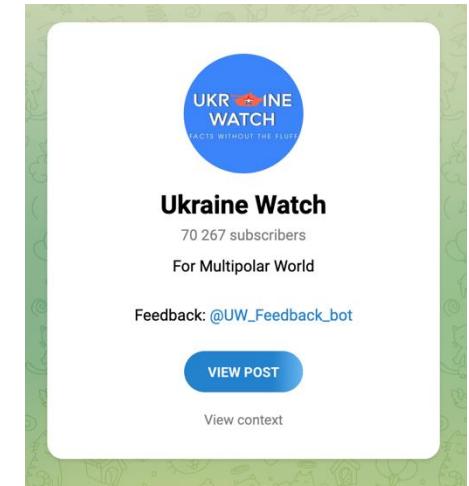


Annulation de la vente de Rafale aux EAU ?

- Arrestation en Fr de Pavel Durov (Telegram). Provoque une reaction officielle des EAU.
- Diffusion et amplification artificielle, vidéo reprenant les codes « Al jazeera ».

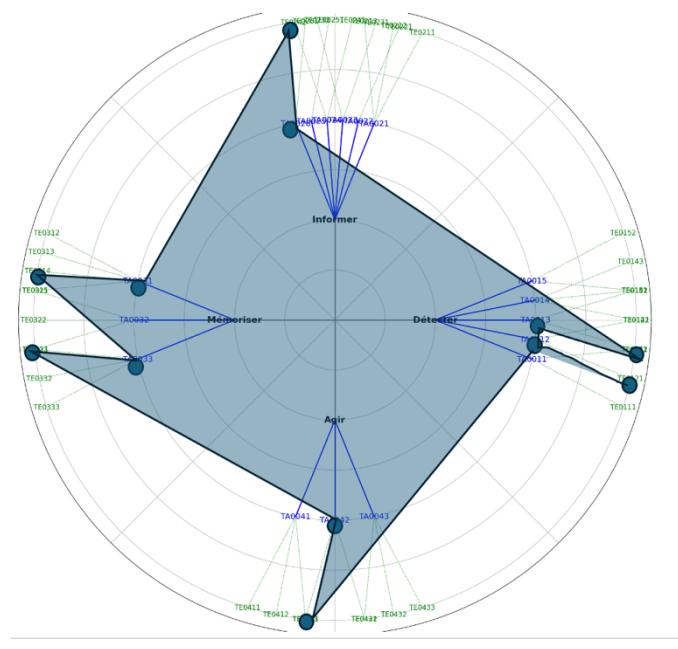


Capture d'écran de la fausse vidéo usurpant le logo d'Al-Jazira et diffusée sur X et Telegram. © X



Analyse DIMA

- **DETECTOR:**
 - TE 0121 « illusion de fréquence »
 - TE0131 : Effet de bizarrie
 - **INFORMER**
 - TE0251: Effet de faux consensus
 - **MEMORISER**
 - TE0312: biais de confusion de source
 - TE0331: Effet de récence
 - **AGIR:**
 - TE 0422 : biais d'autorité



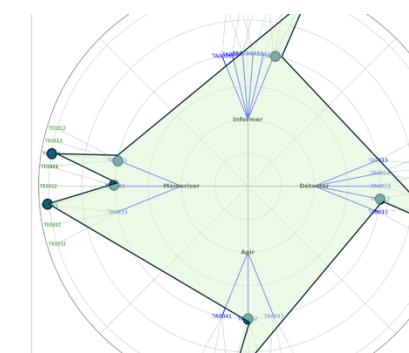
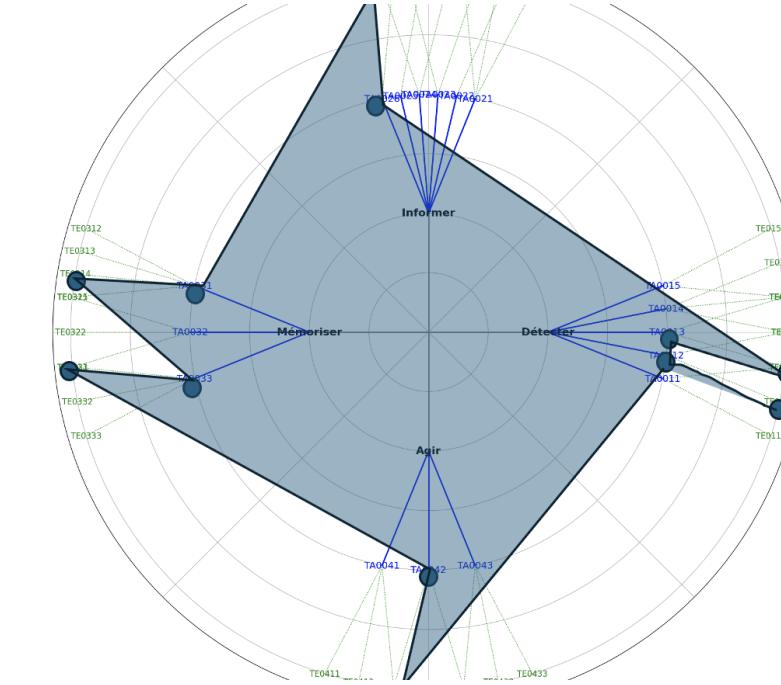
Où allons-nous ?

Analyse des cas documentés (projet DIOD);

Evaluer les similitudes par des décompositions de Fourier et les distances de Hausdorff;

Mesurer l'écart dans le temps de comportement d'un acteur par rapport à un modèle de référence.

Identifier les biais les plus systématiquement exploités par un acteur afin de proposer des mesures de remédiation et de résilience.



Digital Influence Operations Database
sponsored by M82

Outiller DIMA

- Une extension navigateur (**Chrome**)
https://github.com/M82-project/DIMA_Plugin_Chrome
- Une analyse automatique des articles d'un **flux RSS**
<https://github.com/alexbarbaron/DIMAnalyzer>
- Des projets en dév (on ne peut pas en parler mais y'a de l'IA dedans)
<https://github.com/GenerativSchool-Lab/infoverif-extension.git>

Analyse DIMA

Détection de techniques de manipulation cognitive par M82 Project

⚠ Risque élevé
Ce site a été identifié comme diffusant de la désinformation de manière systématique.

Voir les détails du rapport →

19

Score Global

4

Techniques

Modéré

Niveau Risque

2317

Caractères

Analyse par Phase DIMA (Detect, Informer, Mémoriser, Agir)

Analysé : Phase dominante "Detect"

Le contenu utilise principalement des techniques de **détection et captation d'attention** (3/4 techniques). Cela suggère une stratégie axée sur l'identification des publics réceptifs et l'accroche initiale. Le contenu cherche à attirer et cibler des audiences spécifiques.

L'Actualité Provence

Risque élevé
Vigilance : ce site appartient à un dispositif de manipulation de l'information identifié.
En savoir plus →

Rechercher

Messages récents

La campagne de vaccination contre la grippe et le Covid-19 : une mobilisation inquiétante

Philippe Aghion: «Les retraites doivent être suspendues pour empêcher le RN !»

Le président malgache Andry Rajoelina fut le pays sous l'égide d'un avion militaire français en pleine crise de sécurité

Jean-Luc Mélenchon se déclare en faveur du Hamas : une position scandaleuse et répugnante

Victoire retentissante de Pierre-Henri Carbonnel (UDR-RN) dans le Tarn-et-Garonne

Octobre 14, 2025

kherson-news.ru

Site suspect identifié

Risque élevé

Avertissement
Ce site compte à été identifié comme diffusant de la désinformation de manière systématique.

Détails de l'identification

Raison : Poste Portal Kombat ciblé Kherson (Ukraine), amplifiant le ressentiment pro-russe contre les autorités ukrainiennes

Source du rapport : VIBRANT (GOON)

Date d'identification : 03/04/2022

Catégories : Post, Kontakt, Russie, Ukraine, Kherson, Territoires occupés, Désinformation-Cible

Recommandations

Verifiez les informations auprès de sources fiables
Consultez plusieurs sources avant de partager
Soyez attentif aux techniques de manipulation détectées

DIMA FRAMEWORK



Le Framework est en cours de réalisation,



Soutenu par le **M82 project**



Découvrez la matrice sur le framamind :
<https://framindmap.org/c/maps/1457115/public>



Participez au projet :
<https://github.com/M82-project>

