

DIMA

Un *framework* pour décrire les
attaques cognitives



{M}
{82}

De quoi parle-t-on ?

A futuristic robot with glowing blue eyes and a metallic body is holding an open book. The background is a digital space with blue and purple light trails, a large circular structure resembling a satellite or a futuristic building, and a starry sky.

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**.

Pourquoi manipuler l'information ?

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.



Comment ça marche ?

Pour conduire leurs opérations d'influence les acteurs peuvent utiliser des campagnes de manipulation de l'information (mais pas que) des techniques qui exploitent nos biais cognitif et le fonctionnement de notre cerveau.

Les réseaux sociaux sont particulièrement adaptés à la diffusion de campagnes de manipulation de l'information mais pas nécessairement pour les OI ou les « attaques cognitives ».

« 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. »





DIMA

Un framework pour la guerre cognitive

<https://m82-project.org/articles/dima/dima/>
<https://github.com/M82-project/DIMA>

Pourquoi DIMA ?

- Les cerveaux humains, vulnérables aux **biais cognitifs**, sont directement ciblés pour « modifier des comportements ».
- Objectif de la matrice : **Détection et 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.

ATT&CK Matrix for Enterprise

layout: flat ▾

show sub-techniques

hide sub-techniques

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** :
 - Détecter,
 - Donner du sens (informer),
 - Retenir (Mémoriser),
 - Agir.

Reconnaissance

10 techniques

Resource Development

8 techniques

Initial Access

10 techniques

Execution

10 techniques

Persistence

10 techniques

Privilege Escalation

10 techniques

Defense Evasion

43 techniques

Credential Access

17 techniques

Discovery

32 techniques

Lateral Movement

9 techniques

Collection

17 techniques

Communication

18 techniques

Active Scanning (3)

Gather Victim Host Information (4)

Gather Victim Identity Information (3)

Gather Victim Network Information (6)

Gather Victim Org Information (4)

Phishing for Information (4)

Search Closed Sources (2)

Search Open Technical Databases (5)

Search Open Websites/ Domains (3)

Acquire Access

Acquire Infrastructure (8)

Compromise Accounts (3)

Compromise Infrastructure (8)

Develop Capabilities (4)

Establish Accounts (3)

Obtain Capabilities (7)

Stage Capabilities (6)

Content Injection

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (4)

Replication Through Removable Media

Supply Chain Compromise (3)

Trusted Relationship

Valid Accounts (4)

Cloud

Account

Scripting

Container

Exploitation of Client Extensions

Inter-Process Communication

Native API

Scheduled Task/ Job (5)

Serverless Execution

Shared Modules

Software Deployment Tools

System

Account

Boot or Logon

Access Token

Account

Boot or Logon

Boot or Logon

Create or Modify System Process (5)

Create or Modify System Process (3)

Create or Modify System Process (5)

Event Triggered Execution (16)

External Remote Services

Event Triggered Execution (16)

Abuse

Access Token

Account

Boot or Logon

Boot or Logon

Boot or Logon

Create or Modify System Process (5)

Domain or Tenant Policy Modification (2)

Escape to Host

Event Triggered Execution (16)

Exploitation for

Exploitation for

Abuse Elevation

Access Token

Manipulation (5)

Debugger Evasion

Deobfuscate/ Decode Files or Information

Deploy Container

Direct Volume Access

Domain or Tenant Policy Modification (2)

Execution Guardrails (1)

Exploitation for Defense Evasion

Multi-Factor Authentication

Multi-Factor Authentication

Adversary-in-the-Middle (3)

Brute Force (4)

Credentials

Password Stores (6)

Credential Access

Forced Authentication

Forge Web Credentials (2)

Input Capture (4)

Modify Authentication Process (9)

Multi-Factor Authentication

Multi-Factor Authentication

Multi-Factor Authentication

Account Discovery (4)

Application Window Discovery

Browser Information Discovery

Cloud Infrastructure Discovery

Cloud Service Dashboard

Cloud Service Discovery

Cloud Storage Object Discovery

Container and Resource Discovery

Debugger Evasion

Device Driver

Exploitation of Remote Services

Internal Spearphishing

Lateral Tool Transfer

Remote Service Session Hijacking (2)

Remote Services (8)

Replication Through Removable Media

Software Deployment Tools

Taint Shared Content

Use Alternate Authentication Material (4)

Adversary-in-the-Middle (3)

Archive Collected Data (3)

Audio Capture

Automated Collection

Browser Session Hijacking

Clipboard Data

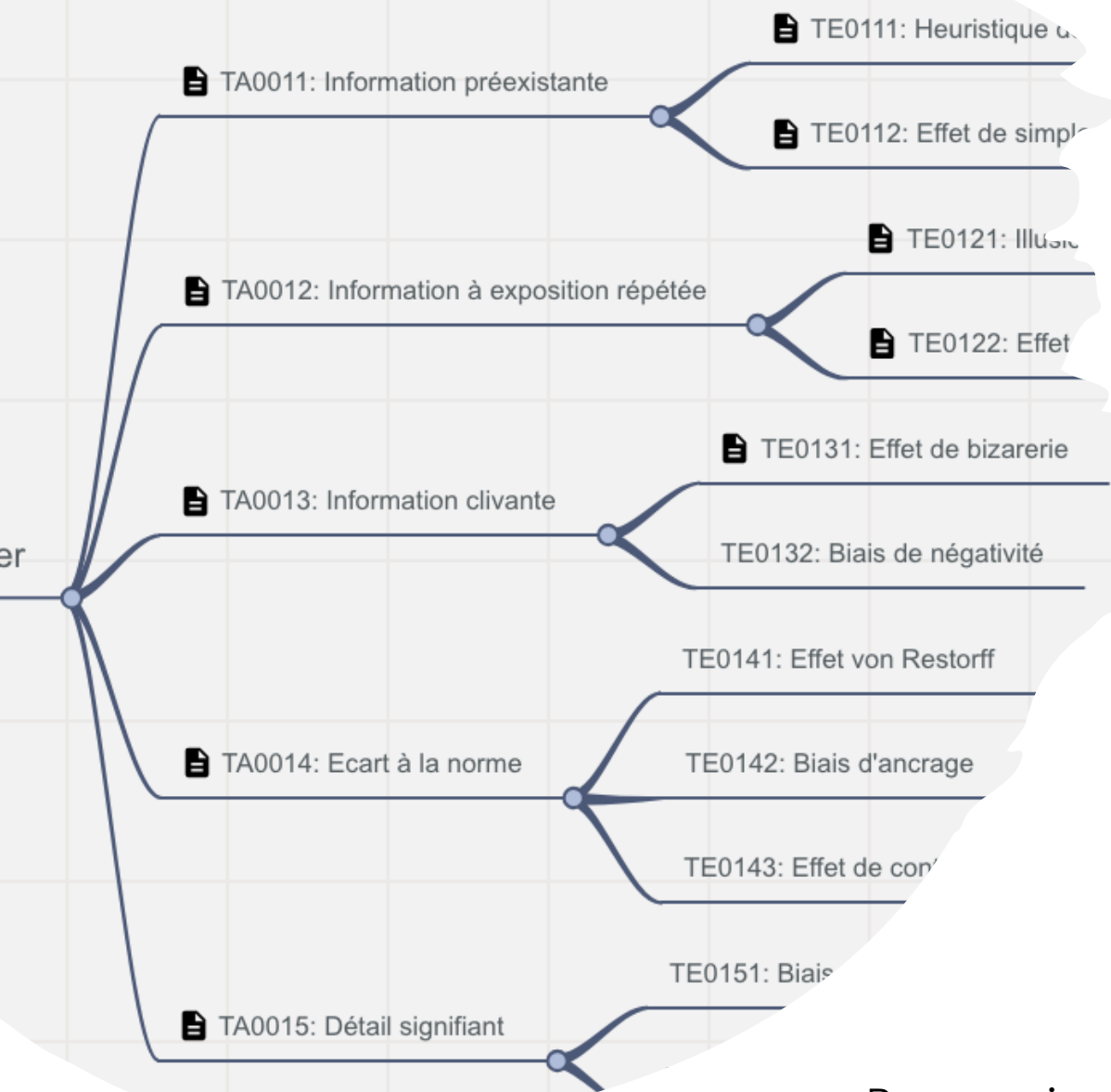
Data from Cloud Storage

Data from Configuration Repository (2)

Data from Information Repositories (3)

Data from Local System

Data from Network Shared



Détecter

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 sélective".

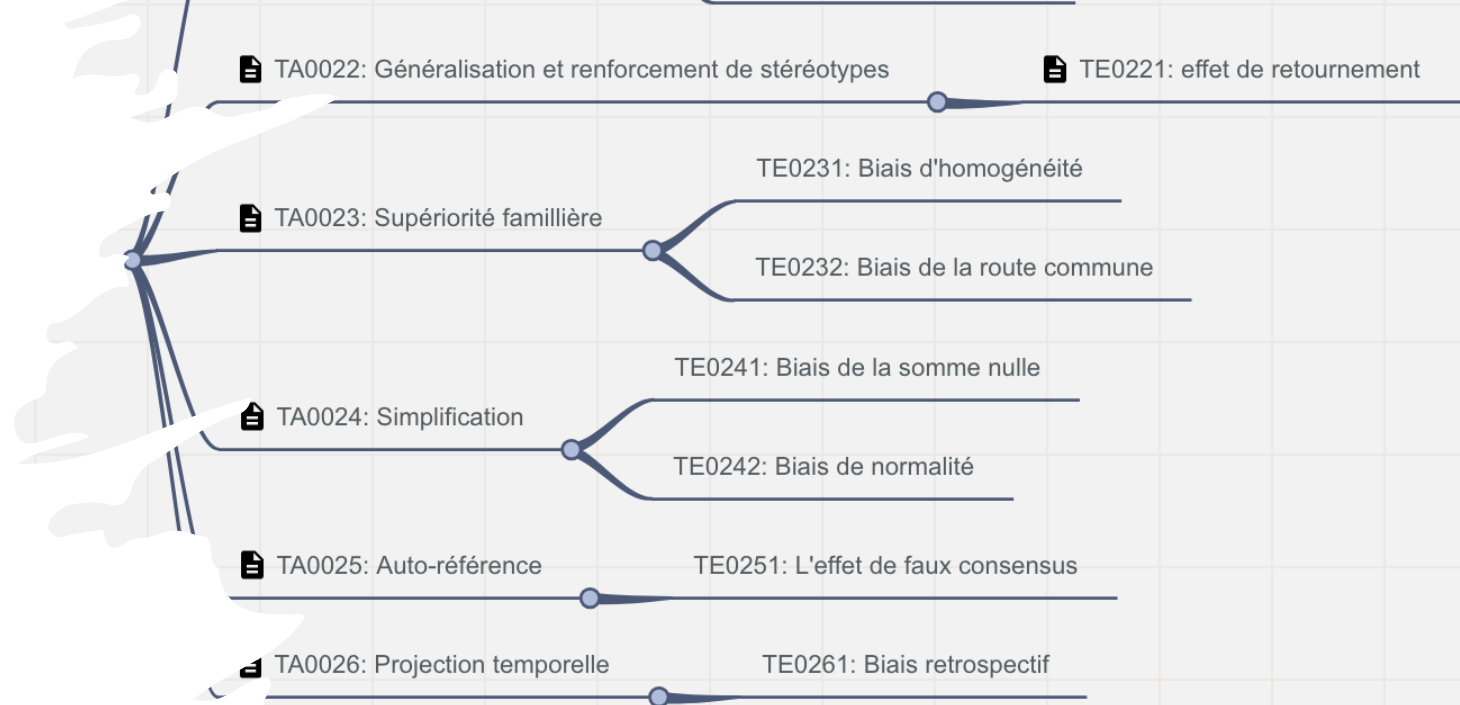
Ce mécanisme est particulièrement à l'œuvre dans la diffusion des thèses complotistes.

"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 »

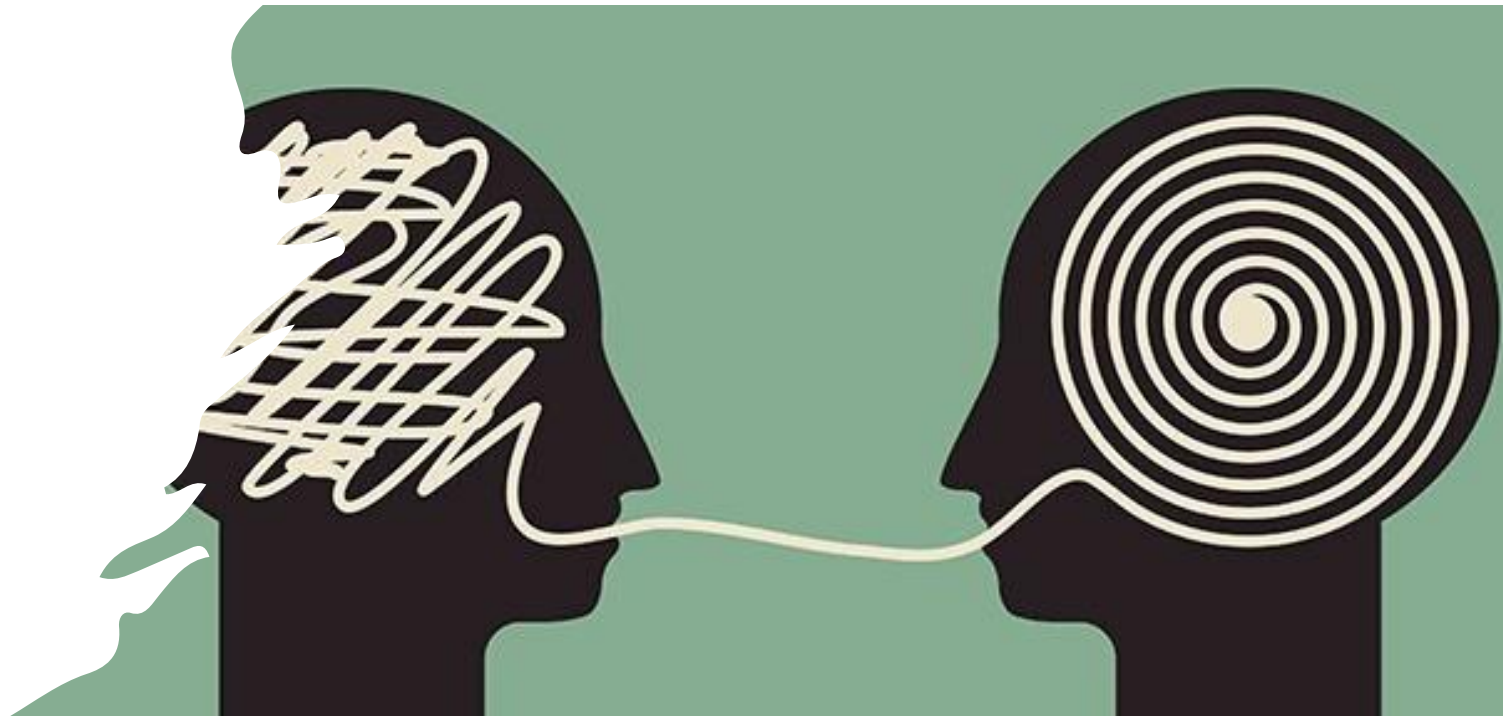
DISARM : T0042 "Seed Kernel of truth"





Informer

POURQUOI CETTE
INFORMATION A UN SENS
POUR MOI ?





Épidémie de parasites Paris : la capitale est sous l'emprise des punaises de lit

Article réservé aux abonnés

Les parasitologues estiment que l'épidémie de punaises de lit à Paris est liée à l'afflux de réfugiés ukrainiens dans la capitale.



Société



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

Par E.P

Mis à jour il y a 8 minutes

Copier le lien



20



Paris Marseille Toulouse Lille Nantes Lyon Bord >

ACCUEIL > PARIS

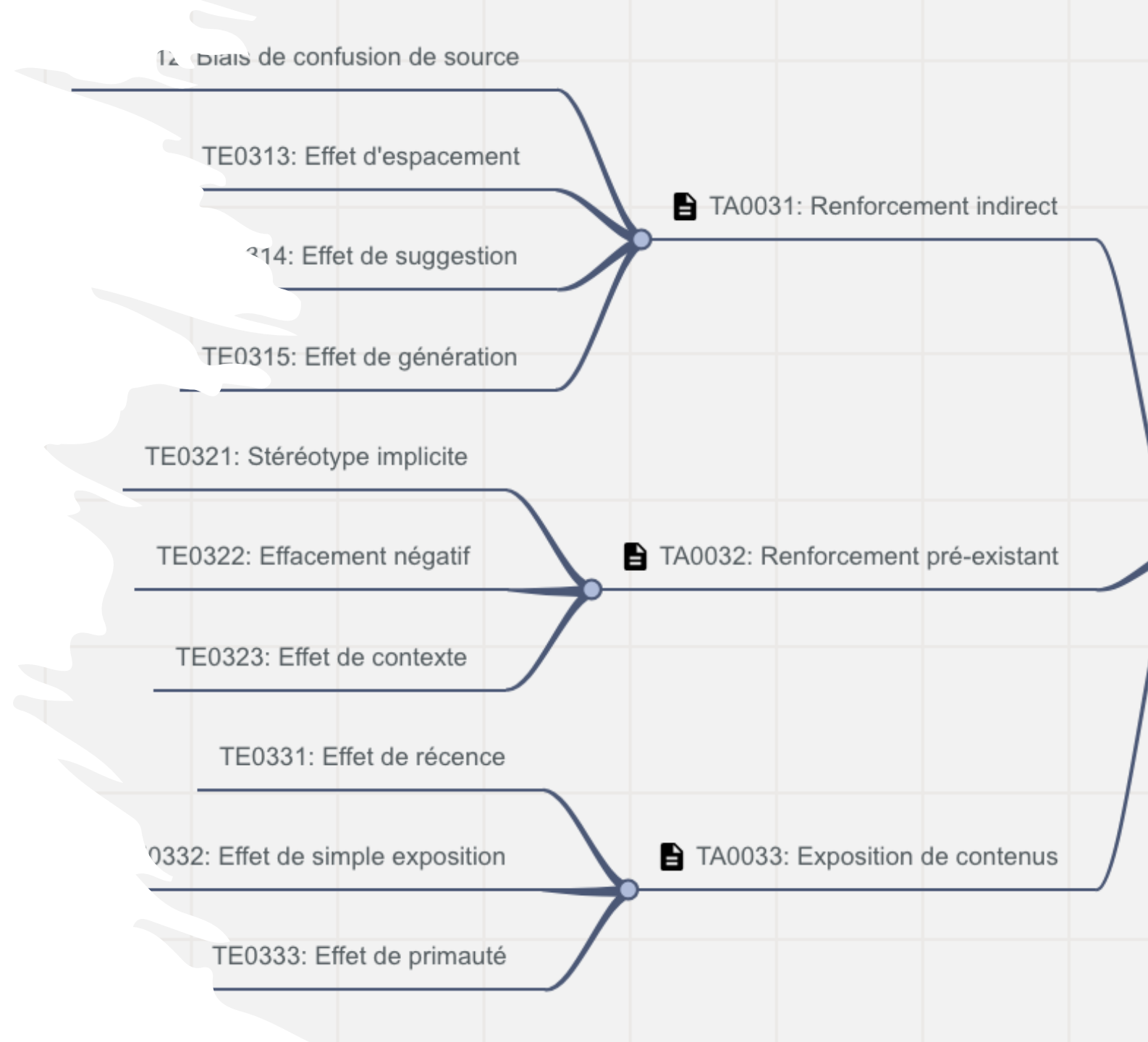


TE 0211: Biais de corrélation illusoire

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

Mémoriser

- Pourquoi retenir cette information ?



TE 0314: effet de suggestion

TE 0321: Stéréotype implicite

- Usage de l'interrogation
- Amplification de stéréotypes



 / Société



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





Agir

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

TE 0422 : biais
d'autorité

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.

 15
COMMENTER

 PARTAGER

 SAUVEGARDER

 UNE FAUTE ?

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

Framework DIMA

Participez au projet

Découvrez le M82_project

Mémoriser

TA0031: Renforcement indirect

- TE0312: Biais de confusion de source
- TE0313: Effet d'espacement
- TE0314: Effet de suggestion
- TE0315: Effet de génération

TA0032: Renforcement pré-existant

- TE0321: Stéréotype implicite
- TE0322: Effacement négatif
- TE0323: Effet de contexte

TA0033: Exposition de contenus

- TE0331: Effet de récence
- TE0332: Effet de simple exposition
- TE0333: Effet de primauté

TA0041: Valorisation individuelle

- TE0411: Biais d'excès de confiance
- TE0412: Effet Peltzman,
- TE0413: Effet de supériorité illusoire

TA0042: Renforcement escalatoire (retour impossible)

- TE0421: Biais des coûts irrécupérables
- TE0422: Biais d'autorité

TA0043: Ozaekomi waza (contrôle par immobilisation)

- TE0431: Biais d'omission
- TE0432: Biais du statu quo

Agir

Détecter

TA0011: Information préexistante

- TE0111: Heuristique de disponibilité
- TE0112: Effet de simple exposition

TA0012: Information à exposition répétée

- TE0121: Illusion de la fréquence
- TE0122: Effet de contexte

TA0013: Information clivante

- TE0131: Effet de bizarrerie
- TE0132: Biais de négativité

TA0014: Ecart à la norme

- TE0141: Effet von Restorff
- TE0142: Biais d'ancrage
- TE0143: Effet de contraste

TA0015: Détail signifiant

- TE0151: Biais de distinction
- TE0152: Loi de Weber-Fechner

Informar

TA0021: Création d'un motif

- TE0211: Biais de corrélation illusoire
- TE0212: Biais de la preuve
- TE0213: Illusion des séries

TA0022: Généralisation et renforcement de stéréotypes

- TE0221: effet de retournement

TA0023: Supériorité familiale

- TE0231: Biais d'homogénéité
- TE0232: Biais de la route commune

TA0024: Simplification

- TE0241: Biais de la somme nulle
- TE0242: Biais de normalité

TA0025: Auto-référence

- TE0251: L'effet de faux consensus

TA0026: Projection temporelle

- TE0261: Biais retrospectif

DIMA FRAMEWORK

- Le Framework est en cours de réalisation,
- Soutenu par le **M82 project**

<https://m82-project.org/articles/dima/dima/>

- Découvrez la matrice sur le framamind :

<https://framindmap.org/c/maps/1457115/public>

- Participez au projet :

<https://github.com/M82-project/DIMA>

