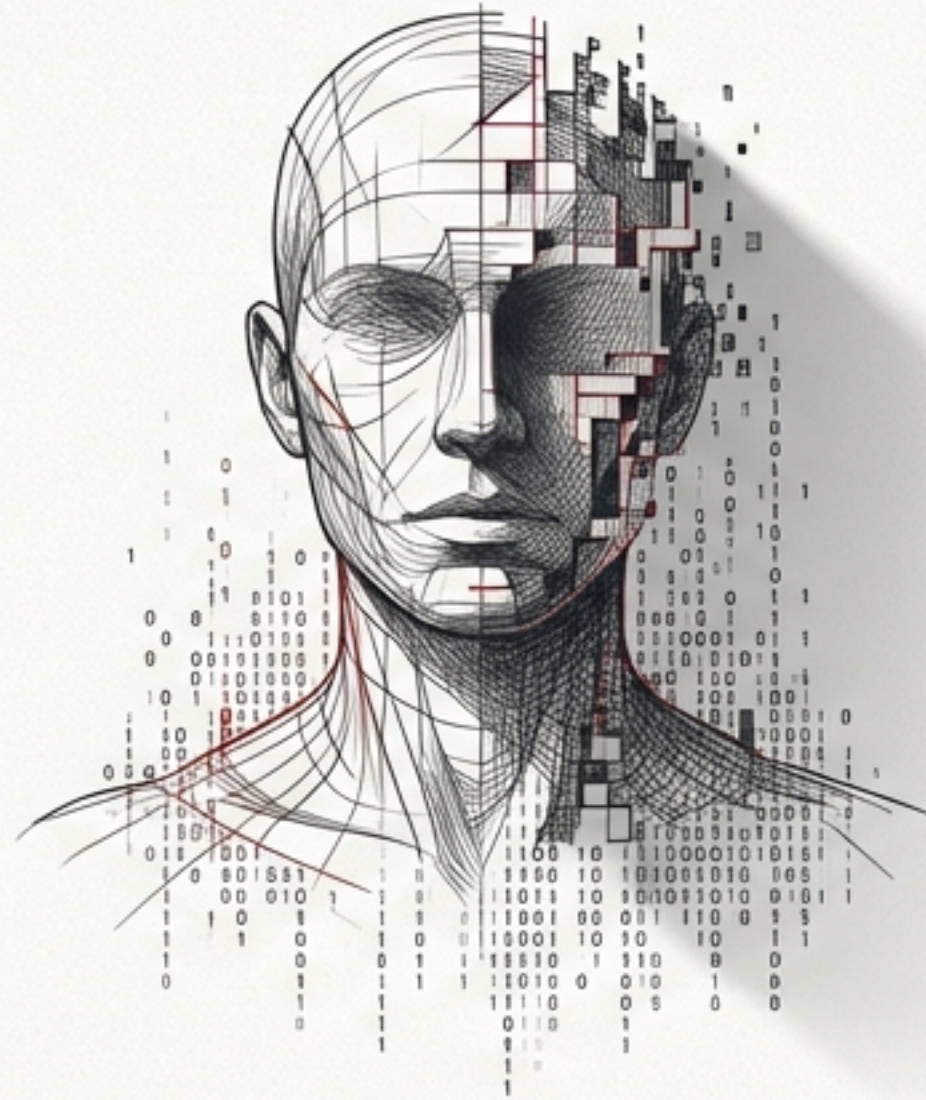


La Guerre sans Visage



Cyberguerre, Influence et Infox : Comprendre
les Conflits de l'Ère Numérique

Une Nouvelle Ère de Conflictualité

La conflictualité se déplace dans un espace où l'on ne voit pas toujours l'attaquant, ni même le moment exact où la guerre commence.



Le Mécanisme-Clé : Le Problème d'Attribution

Définition : Prouver « qui » est responsable d'une attaque est un processus long, techniquement incertain et politiquement contestable.

Conséquence : Ce brouillard structurel rend la dissuasion classique inefficace.

Le Lexique de la Guerre Numérique

Il est essentiel de distinguer les motivations et les objectifs pour ne pas tout qualifier de « cyberguerre ».



Cyberguerre

Usage d'opérations numériques par des acteurs étatiques pour atteindre des objectifs stratégiques (espionner, perturber, détruire).



Cybercriminalité

Motivée principalement par le profit (fraudes, rançons).



Cyberespionnage

Focalisé sur le vol de renseignement (données, secrets industriels).



Cybersabotage

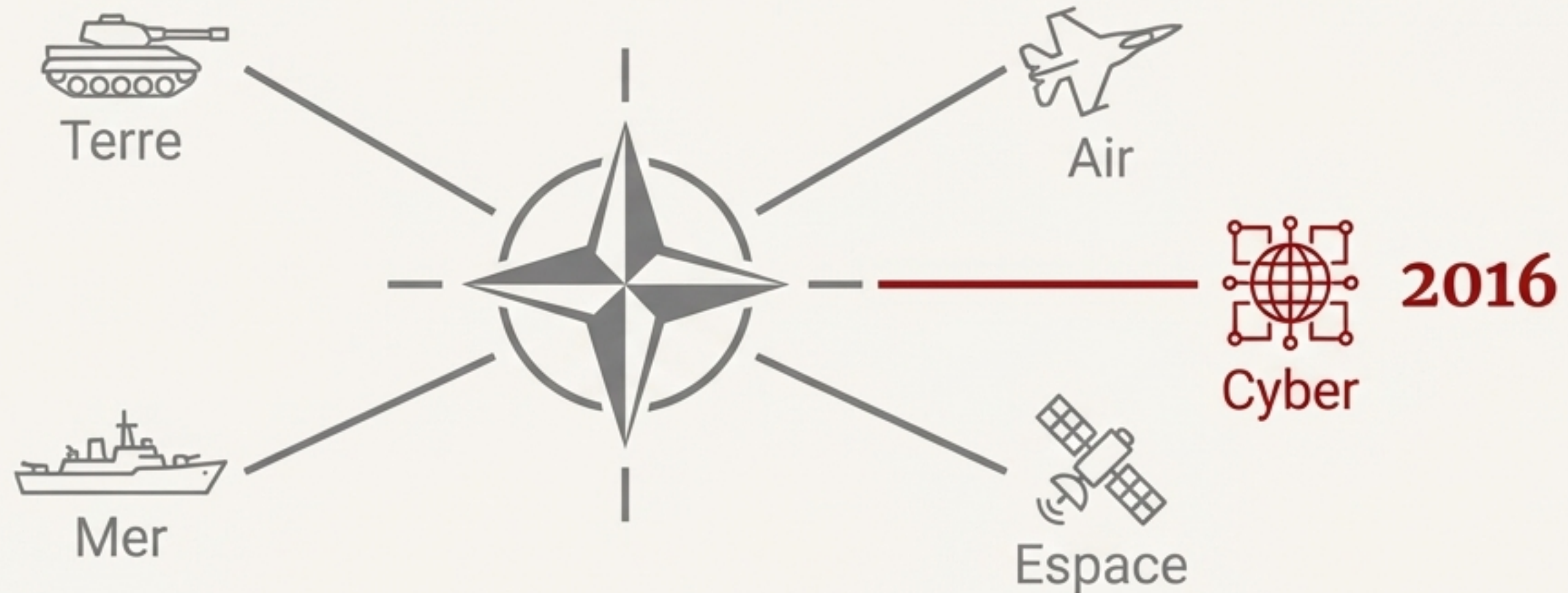
Vise à créer des dommages physiques et des perturbations de services.



Influence / FIMI

Manipulation des perceptions, polarisation, démobilisation. Vise l'esprit, pas les systèmes.

2016 : Le Cyber devient un Théâtre d'Opérations Stratégiques



Repère institutionnel clé

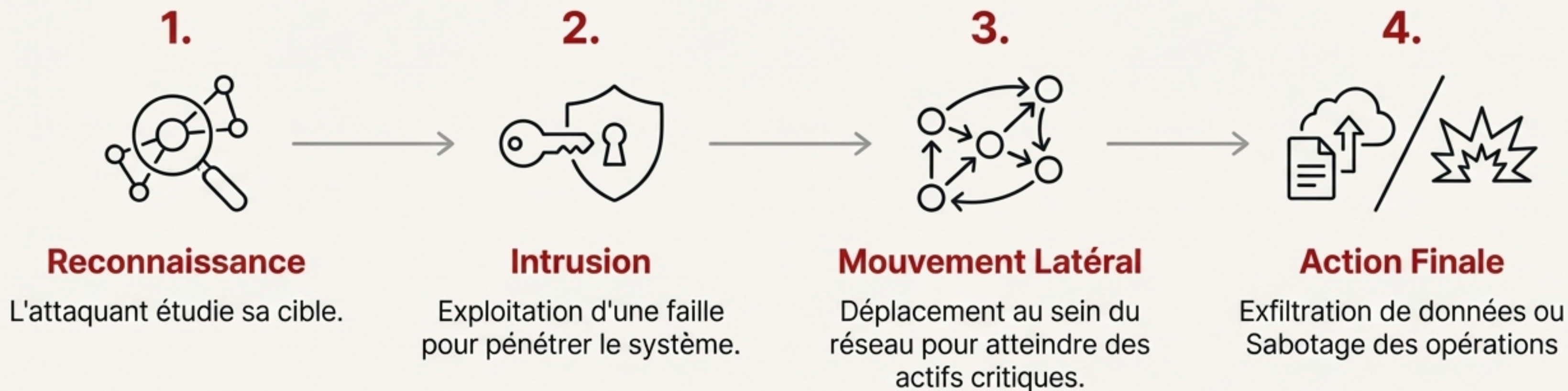
L'OTAN reconnaît le cyberspace comme un domaine opérationnel, au même titre que la terre, l'air, la mer et l'espace.

Implication stratégique

Le cyber n'est plus un problème purement technique, mais un enjeu de défense collective.

« Cyber defence is part of NATO's core task of collective defence. »

Anatomie d'une Cyberattaque : La Chaîne Technique



Vulnérabilités Ciblées



Failles logicielles (logiciels non mis à jour).



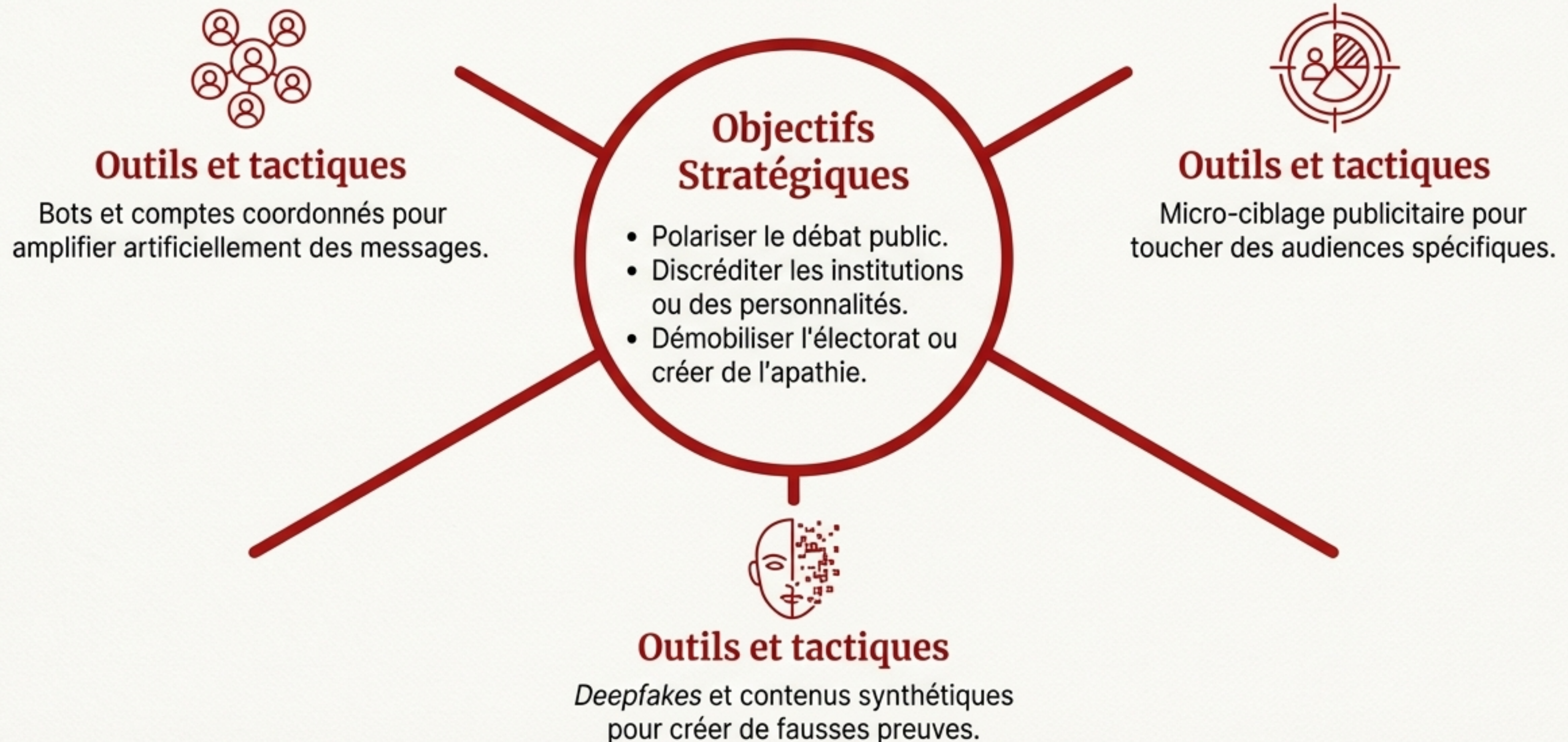
Erreurs humaines (phishing, mots de passe faibles).



Dépendances à des prestataires (*supply chain*).

Anatomie d'une Opération d'Influence : La Chaîne Informationnelle

Concept de référence : **FIMI** (Foreign Information Manipulation and Interference) - Notion utilisée par l'UE pour désigner les opérations coordonnées visant à manipuler l'information à des fins politiques.



2017-2020 : Les Attaques qui ont Redéfini la Menace



WannaCry (Mai 2017)

Type : Ransomware à impact massif.

Leçon : A exposé la vulnérabilité critique des services publics, notamment le système de santé britannique (NHS).



NotPetya (Juin 2017)

Type : Attaque destructrice déguisée en ransomware.

Leçon : A démontré le potentiel de paralysie économique mondiale. Coût estimé :

≈ 10 milliards de dollars



SolarWinds (Révélé en Déc. 2020)

Type : Compromission de la chaîne d'approvisionnement (*supply chain*).

Leçon : A illustré la difficulté extrême de se défendre quand un tiers de confiance est infiltré.

Riposter dans le Brouillard : Le Défi de la Dissuasion

Le problème : La dissuasion classique (« par punition ») est inefficace car l'attaquant est souvent caché, rendant la menace de riposte peu crédible.

Dissuasion par Punition	La nouvelle doctrine : Dissuasion par Dén
	

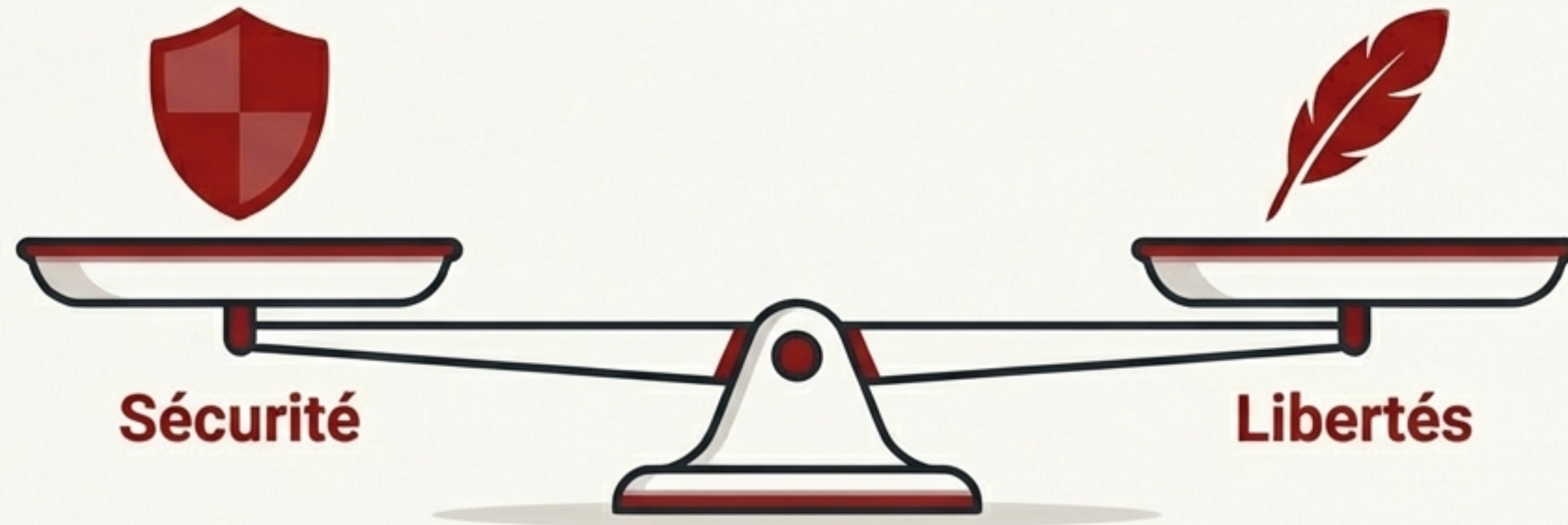
Objectif : Rendre l'attaque inefficace ou si coûteuse pour l'attaquant qu'il y renonce. Il ne s'agit pas de punir, mais de rendre l'effort vain.

Méthodes concrètes :

- **Résilience** : Capacité à continuer de fonctionner malgré une attaque.
- **Hygiène cyber** : Mises à jour (patch), authentification forte.
- **Architecture de défense** : Segmentation des réseaux, sauvegardes régulières et déconnectées.

Les Nouveaux Arbitrages Démocratiques

La lutte contre les menaces numériques crée des tensions fondamentales avec nos valeurs. Il n'y a pas de solution simple.



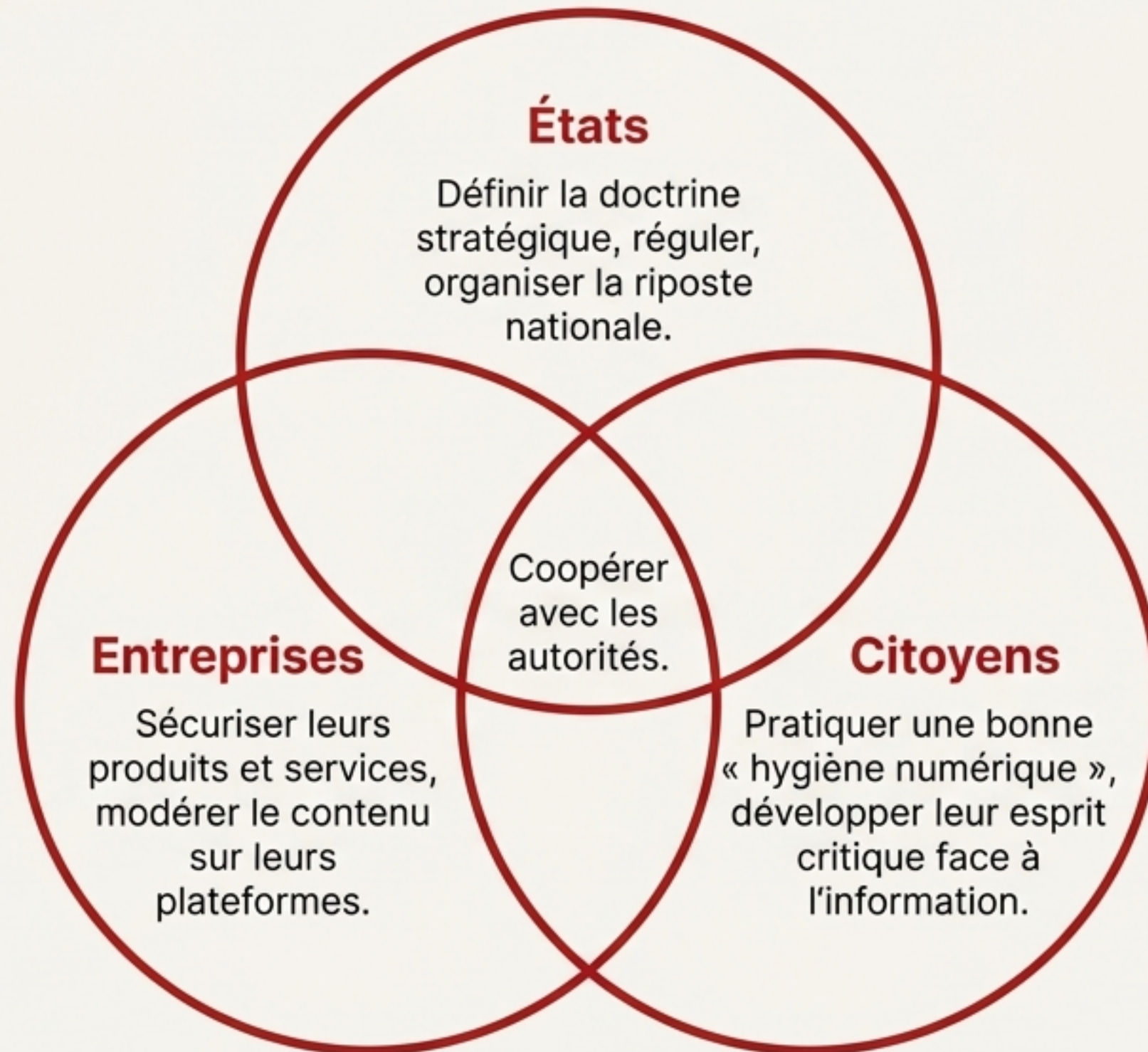
Les Débats Centraux

Sécurité vs Liberté d'expression : Où placer la frontière entre la modération nécessaire de la désinformation et une censure qui menacerait le débat public ?

Guerre vs Criminalité : Faut-il traiter les cyberattaques majeures comme des actes de guerre (réponse militaire) ou comme une forme de criminalité sophistiquée (réponse judiciaire) ?

La Sécurité Numérique : Une Responsabilité Partagée

Qui doit payer pour la sécurité et comment gérer les interdépendances dans un monde hyper-connecté ?



Prochaine Frontière : L'IA Générative, Accélérateur de Crise

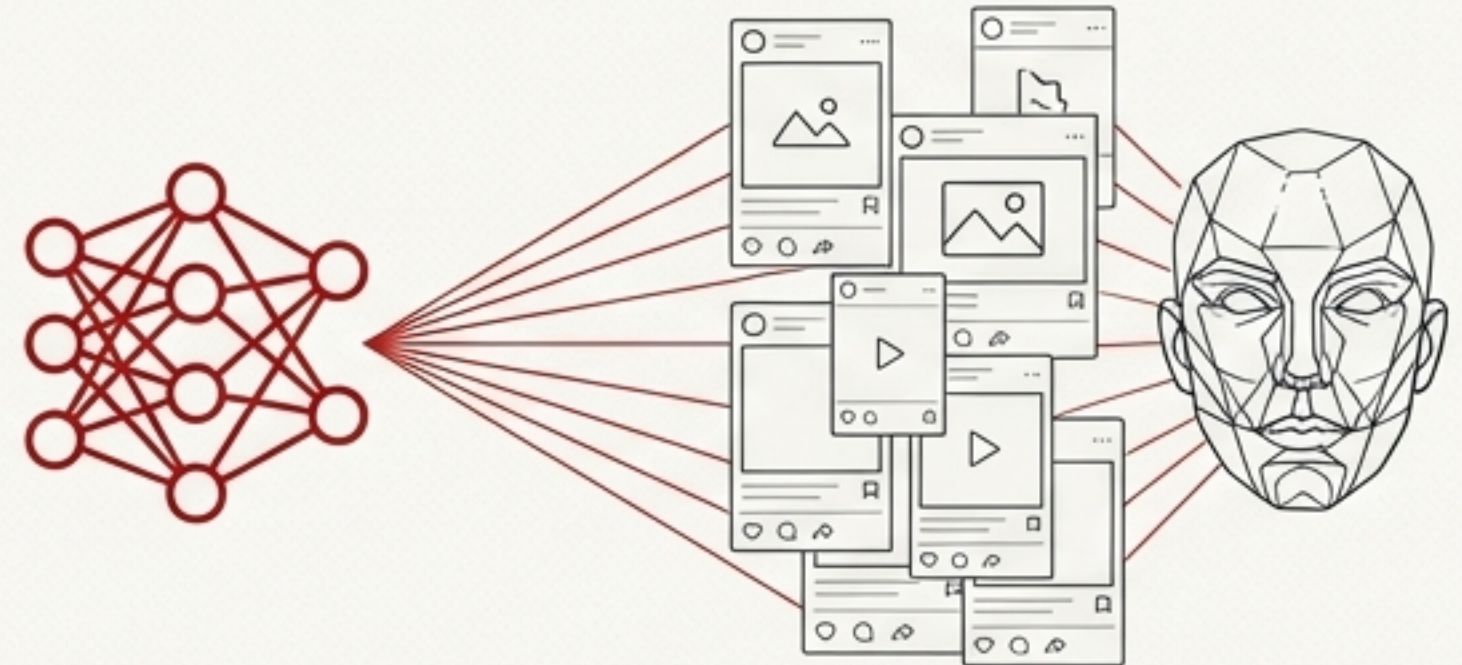
L'IA générative n'est pas une nouvelle menace en soi, mais un amplificateur massif des menaces existantes.

Défense améliorée



Détection plus rapide des anomalies et des campagnes d'influence.

Menace amplifiée



Production de désinformation et de *deepfakes* sophistiqués à très grande échelle et à coût quasi nul.
Personnalisation des attaques de phishing.

La Question Centrale pour l'Avenir : **L'IA va-t-elle fragiliser la confiance démocratique au point de rupture ?**

Grille de Lecture Stratégique : Les Pièges à Éviter



[X] Le piège du tout-'cyberguerre'

Toujours distinguer criminalité (profit), espionnage (renseignement) et sabotage (destruction).



[X] Le piège techno-solutionniste

Ne pas croire que la technique seule suffit. La cyberdéfense est aussi une question de gouvernance, de budget, de formation et de culture.



[X] L'oubli de l'attribution

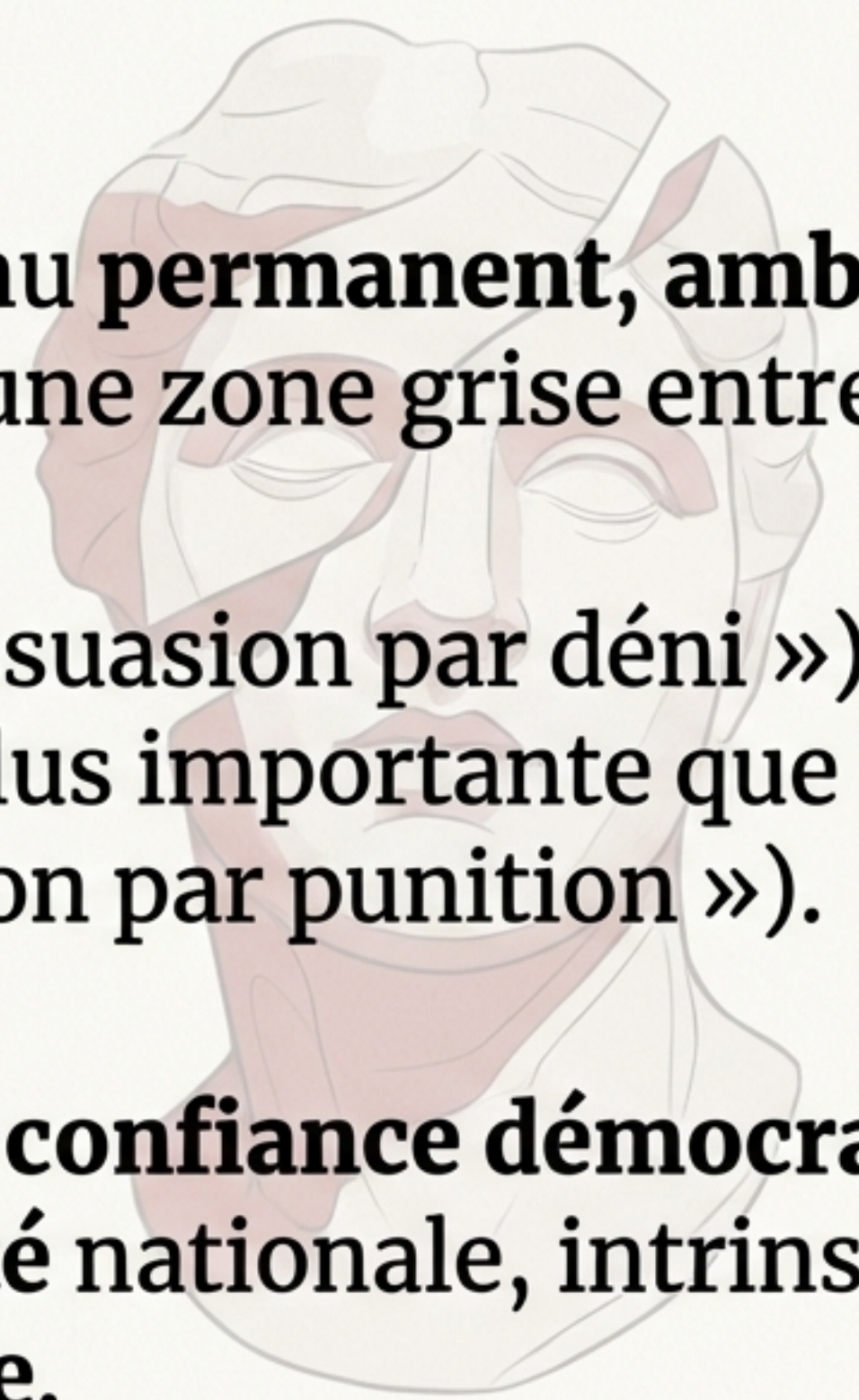
Garder à l'esprit que sans attribution crédible, **toute riposte** politique est fragile et risquée.



[X] La confusion sémantique

Distinguer la **désinformation** (intention de nuire) de la **mésinformation** ou de l'erreur (pas d'intention malveillante).

La Nouvelle Réalité Stratégique du XXI^e Siècle

- 
1. Le conflit est devenu **permanent, ambigu et informationnel**, se déroulant dans une zone grise entre la paix et la guerre.
 2. La **résilience** (« dissuasion par déni ») est devenue stratégiquement plus importante que la seule capacité de riposte (« dissuasion par punition »).
 3. La protection de la **confiance démocratique** est désormais un enjeu de sécurité nationale, intrinsèquement lié à la sécurité numérique.

Sources et Pour Aller Plus Loin

Sources Institutionnelles de Référence

Foreign Information Manipulation and Interference (**FIMI**) – EEAS (Service européen pour l'action extérieure)

FIMI and Cyber Threat Intelligence – ENISA (Agence de l'UE pour la cybersécurité)

Cyber defence – NATO (Organisation du traité de l'Atlantique nord)

SolarWinds Orion Compromise – CISA (Cybersecurity and Infrastructure Security Agency, USA)

Analyses et Ouvrages

The NotPetya Attack – Brookings Institution

The Age of Surveillance Capitalism – **Shoshana Zuboff**

The Road to Unfreedom – Timothy Snyder