La prédation informationnelle

Un couteau suisse, une forme de « domination » humaine / économique / stratégique

Présentation RESIST 20 juin 2017 / Teyssier Damien

L’information, le vrai carburant du monde ?

constituant essentiel professionnel et personnel

Impact individuel / interpersonnel

Impact collectif / sociétal

Mais nous avons un problème

Nous ne « récupérons » directement pas les informations du monde qui nous entoure

nous les percevons ou non (sens) puis les filtrons, intentionnellement ou non, avant de les exploiter

En plus, l'évolution technique a modifié nos méthodes individuelles et collectives d'acquisition d'info.

- on n'apprend ou fait apprendre,
- on perçoit ou fait percevoir,
- on fait ou fait faire,
- on croit ou fait croire,

de manière différente que durant les années 80

Cela induit de nouvelles formes de domination

- acquisition d'une supériorité ou d'un profit par l'information,
- « *prédation* » informationnelle,
- contrôle des perceptions ou connaissances, d'une victime,

mais aussi de destruction et de chaos

- paralysie d'infrastructures techniques,
- désinformation ou dénigrement,
- atteinte à l'intégrité des mémoires ou des systèmes d'information,
- acquisition, altération ou rétention des connaissances à l'aide de machines à stocker, traiter ou propager des informations

Ce sont ces processus d'acquisition / traitement que les prédateurs informationnels vont cibler pour atteindre leur(s) objectif(s):

Collecter de l'information provenant de sources humaines
en exploitant les failles de ce maillon, techniquement ou non,
dans le but d'acquérir une supériorité ou un profit

Mais qui sont ces prédateurs ?

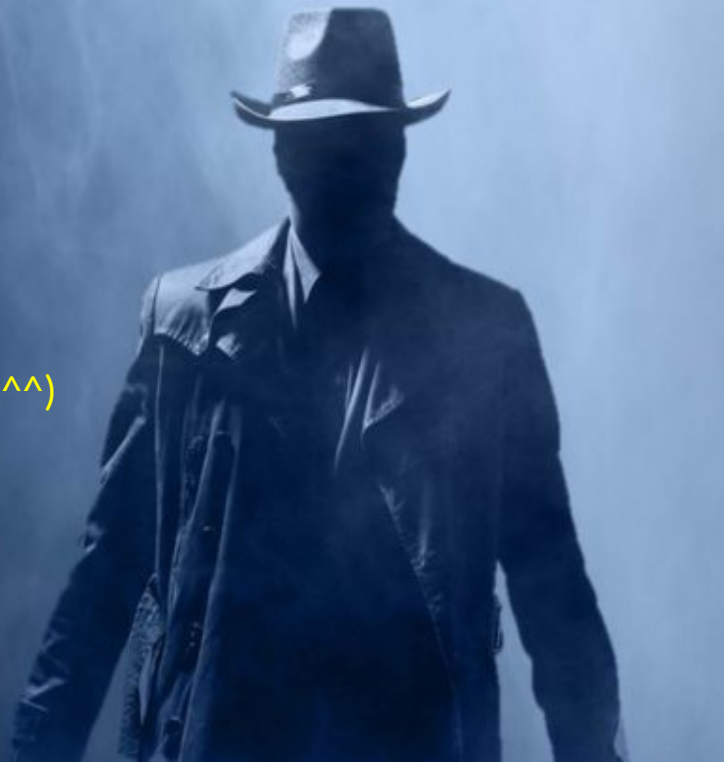
La prédation info est ancrée en nous, c'est la 1ere relation sociale !
Nous sommes donc tous des prédateurs…

Certains le sont cependant en plus à titre professionnel:

- **Les arnaqueurs**
- **Les Social Engineers**

} Souvent peu formés (heureusement^^)

- **Les officers traitants (rens. offensif)**
- **Le perception modeller**
- **Le désinformateur**
- **L'expert en guerre de l'information**



Méthodologie de récupération d'information

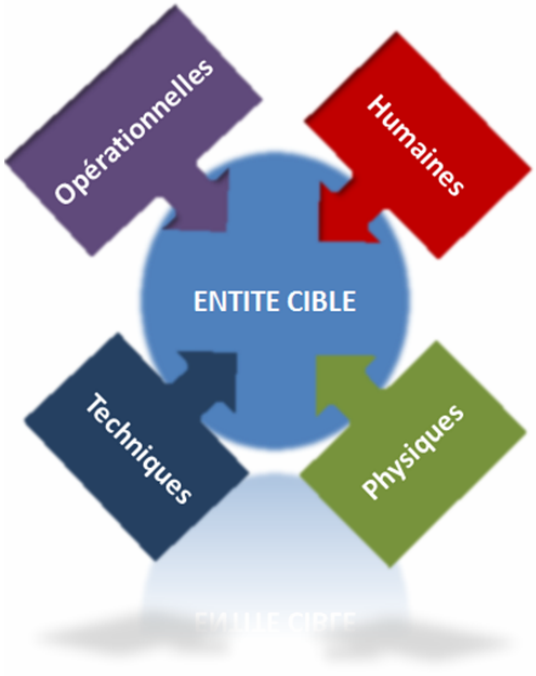
1. L'identification de failles
2. L'identification des cibles (individus)
3. Exploitation des failles

Nous verrons ensuite comment nous protéger

Pour terminer, nous verrons comment détourner certaines techniques:

Utilisation positive et éthique
(management, RSSI, formation, gestion RH,…)

L'identification de failles



4 types de failles

les failles opérationnelles (activités régulières de l'entreprise):

- prédictibilité des opérations et procédures de mise en œuvre,
- faibles procédures de défense,
- Activités extérieures, contractants, outsourcing,…
- Recherche d'efficience qui facilite l'attaque en profondeur
- Fragilité de services (marketing, comm, RH, relations publiques,…)

les failles physiques:

- Points de contrôle faibles ou absents
- Analyse de l'environnement physique extérieurs (parking, poubelle,…) pour en tirer des infos
- Bureaux mal rangés, réunions dans des zones regroupant plein d'infos, TEMPEST,…
- Dépannage sur site (pour voler la mémoire du copieur par exemple,…)
- Accès non ou mal sécurisés

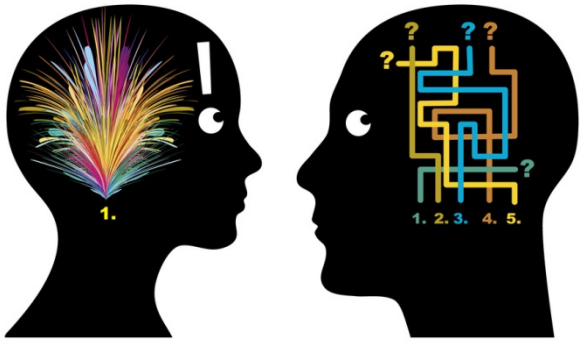
les failles techniques:

par technique nous entendons l'ensemble des failles pouvant être exploitées par un mode technique:

- Pénétration informatique

Les principales failles dans cette catégorie sont : les failles logicielles, erreurs de configuration ; la gestion des passwords ; le stockage des archives ; les canaux de transmission (interne/externe) de l'information ;

- Surveillance électronique (tempest, EMP, IMSI catcher,…)



Les failles humaines

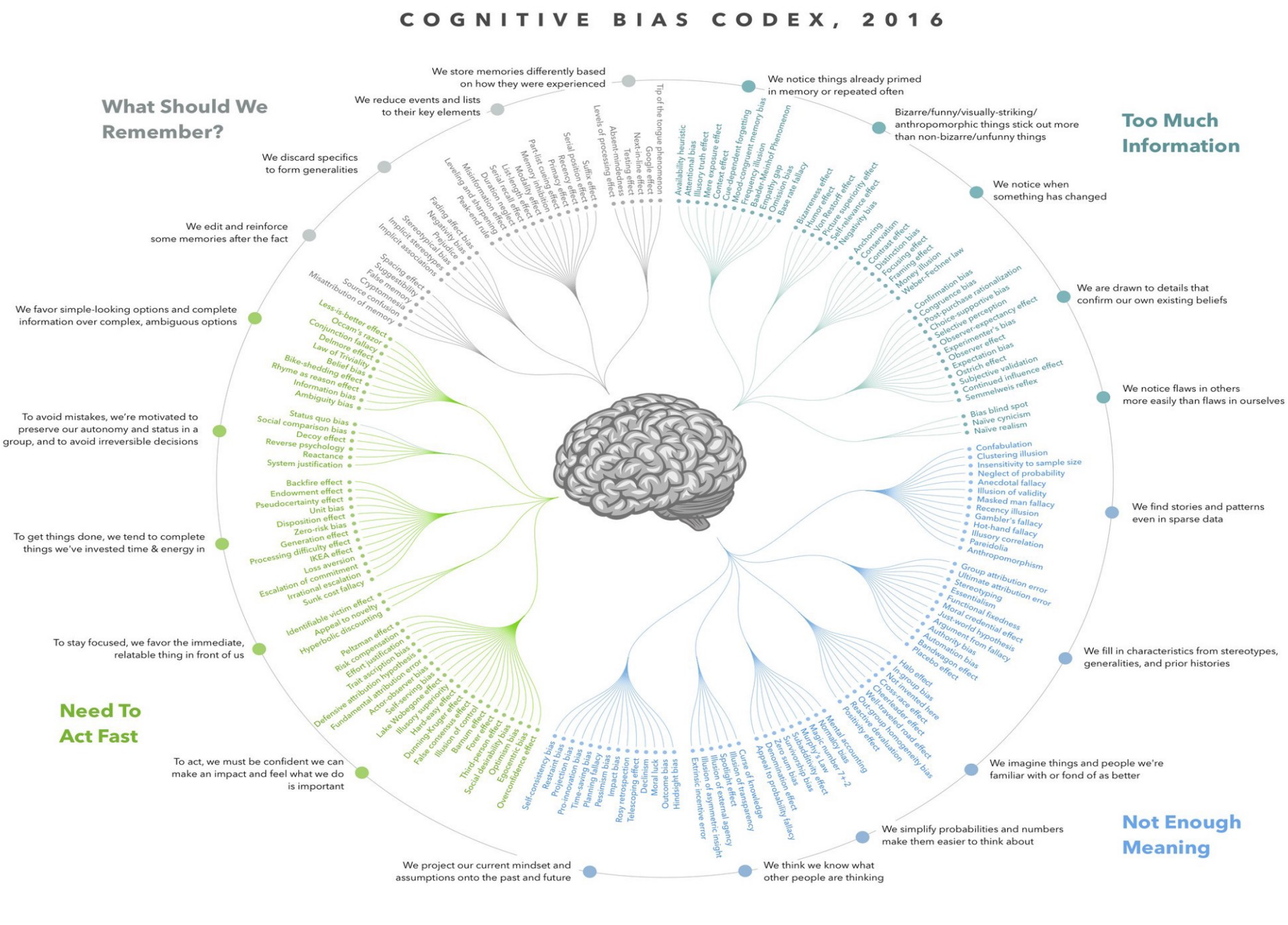
Je ne pourrai pas tout expliciter pour des raisons que vous comprendrez, mais nous pouvons parler de:

- Biais cognitifs / heuristiques

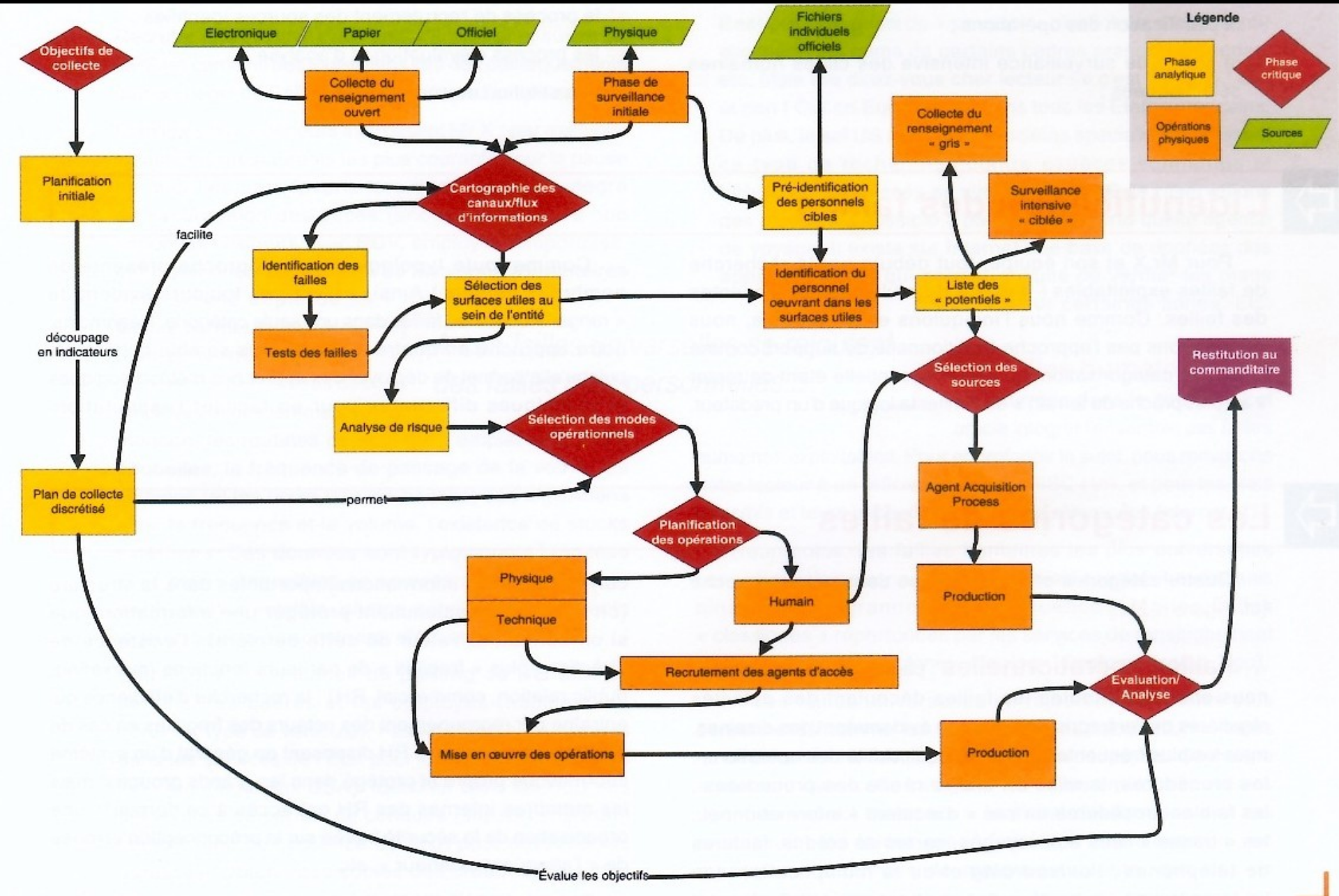
- Cold reading (sorte d'outil statistiqu es), VAKO et autres méthodes non verbales
- Elicitation, recrutement de sources,…
- Techniques de manipulation ou de persuation telles que:
  - MICE: Money/Ideology/Compromission/Ego
  - SANSOUCIS : Solitude, Argent, Nouveauté, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance)
  - L'ELM: Elaboration Likehood Model : voie centrale (motivation initiale) et voie périphérique (variation de la forme des msg)
- Phases de fragilité (divorces, plans sociaux, harcèlement, responsabilités complexes, problèmes financiers,…)

- Absence de barrières informationnelles (Chinese wall)
- Radio machine à café, radio lavabo,…
- Profilage structurel de traits visibles lors d'interactions humaines (Big 5, MBTI par exemple) ou d'autres types de profilage orientés différemment (RIASEC, …)

Exemple des biais cognitifs: certains sont opérationnels, d'autres théoriques



Choix de la cible et Xploit des failles



Quelques détails à noter

- Connaissance des lieux, des horaires, des prestataires, des sites,…
- Cartographier la cible (flux entrants, sortants, organigramme inversé, carte des process…)
- Faire une analyse multidimensionnelle permet de « superposer » les cartographies avec d'autres analyses, qui permettent de définir les surfaces utiles, humaines ou non.
- Faire un SNA (social network analysis): permet de savoir qui est proche de qui ou qui n'aime pas qui ^^. On peut tagger aussi les électrons libres, les « ouverts sur le monde »,…
- Faire une matrice des risques, car la 1ere règle d'un prédateur,

c'est ne pas se faire détecter, ne pas se faire attraper…

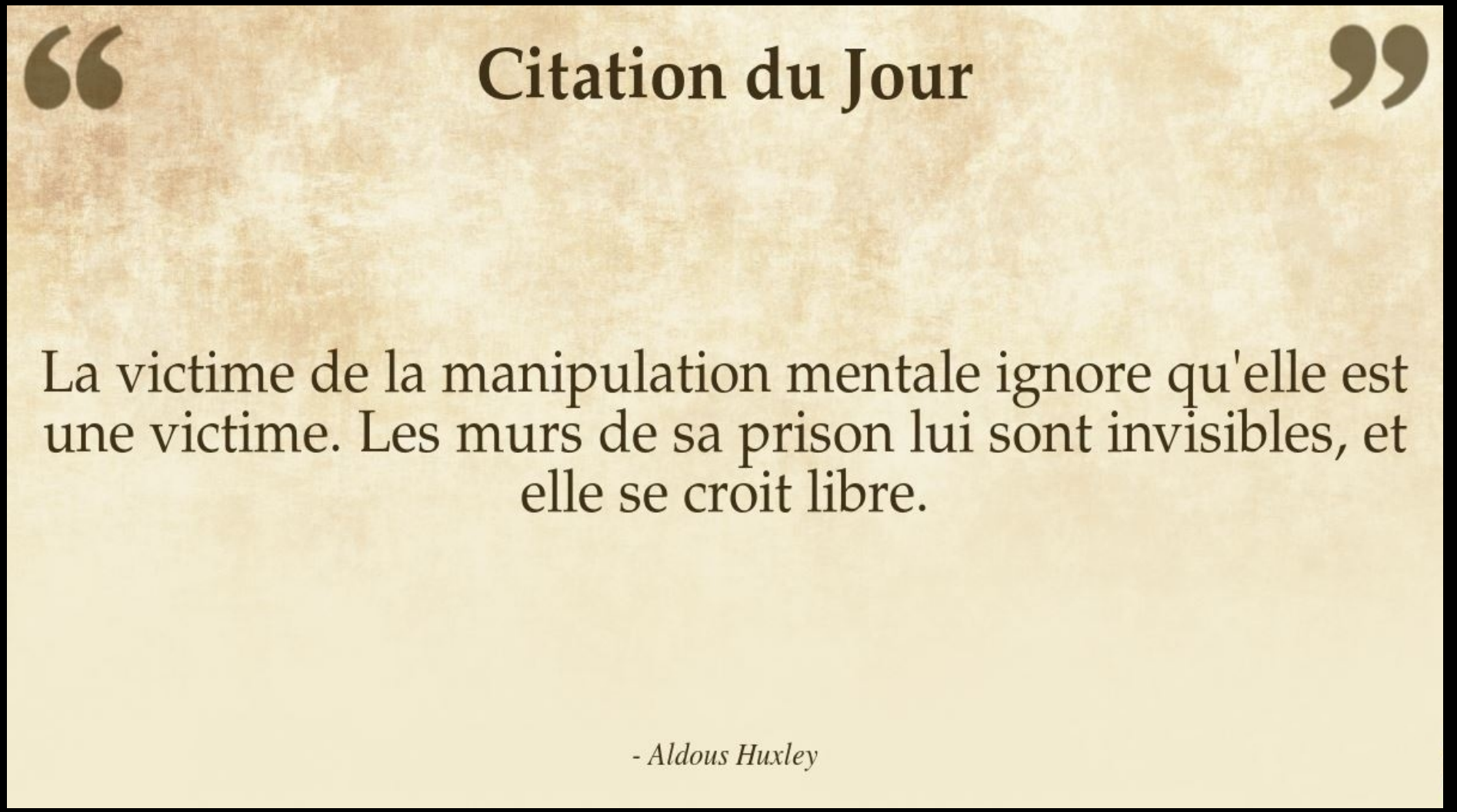
La prédation informationnelle, c'est une forme d'APT non technique

Dans cette analyse, on notera les risques de raté, les types de protection, le degré de capacité d'analyse, d'intervention de la cible, la logistique, les risques physiques, techniques,…

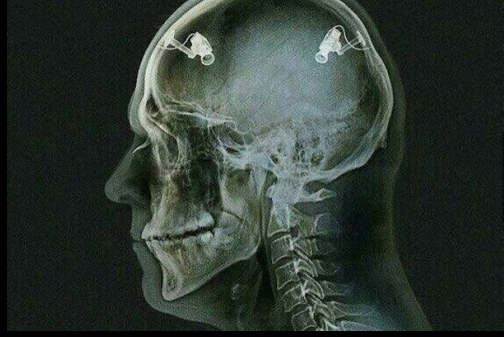
Un petit jeu ?

Dans cette vidéo, l'action tentée à fonctionné 2 fois. Comment ?

Pourquoi échoue-t-elle sur le vendeur de hot-dog?



Comment se protéger



C’est possible !

- Créer des procédures d’alerte spécifiques pour générer, auprès d’un « concentrateur » bien formé , un ou des Early Warning (faisant passer les personnels concernés en « système 2 »).
- Mettre en place des procédures techniques qui tiennent compte des biais et limite leur impact ou augmente les risques de détection: double signature, cloaking (perception management des projets,,…)
- Surveiller les informations qui sortent de chez nous avec une vision « offensive »
- Déployer des procédures de gestion en cas d’early warning, déployer une méthodologie de management intégrant ces risques
- Bien entendu, former les gens (exercices spécifiques, red team humain à minima, global si possible,…)
- Former les gens à réagir correctement lorsqu’ils ont le sentiment d’être élicités !

Utiliser la prédation autrement

On peut utiliser certaines techniques (profilage relationnel, connaissance des biais métiers,…) pour améliorer entre autre son management et toutes ses relations interpersonnelles (pro ou non).

Exemples:

- Connaitre les biais majeurs métiers permet de mieux comprendre les réactions de ses collaborateurs et donc de mieux interagir.

En effet, un biais n'est pas de de l'incompétence, de la mauvaise foi ou du manque d'expérience. Il s'agit d'un mécanisme complètement inconscient, automatique et qui frappe tout individu de la même manière.

⇒ On peut aussi travailler sur soi (eh oui, on en a plein de failles !!) en intégrant certains process (self management mental / procédural, métier ou personnel)

⇒ On peut aussi améliorer son team building en créant des équipes cohérentes techniquement mais aussi au plan humain.

⇒ On peut améliorer ses méthodes de formation en tenant compte des biais, et dans le cadre de la sécu, de la prédation informationnelle dans son ensemble. On peut du coup s'entrainer mieux et plus souvent, par le biais de petits jeux par exemple…

⇒ On peut repenser son organisation, son environnement, avec une vision plus cohérente des risques (intelligence économique, stratégique,…)

⇒ On se perçoit différemment, et cela change déjà TOUT ! (l'égo est un ennemi puissant)

Quelques biais de managers, en êtes vous victimes ?

Biais de disponibilité: tendance à évaluer une proba. en se basant sur nos exemples en mémoire

Biais de cadrage: tendance à interpréter et à réagir différemment selon si l'info est présentée comme un gain ou une perte.

Biais d'ancrage: tendance à s'appuyer sur une référence passée pour prendre une décision

Biais d'expertise: tendance à attribuer un degré d'expertise à des personnes avec une position sociale qu'on imagine supérieure en terme de savoir, intelligence,…

Biais d'objectivité: tendance à percevoir les gens objectifs comme plus crédibles que les autres

Biais de similarité: il me ressemble (valeurs, attitudes, opinions,…), donc il est crédible ;)

Illusion de validité: tendance à croire que des données répétées et cohérentes possèdent une vraie valeur prédictive (sur-évalution)

Effet de Halo: tendance à voir un trait positif ou négatif impacter totalement notre vision de la personne

Si vous saviez « corriger » ou contrebalancer ces quelques traits, cela changerait votre perception métier et vos actions ? Mieux ou pas ?

Merci de m’avoir laissé manipuler votre attention aussi longtemps ;)

Sources : Michel Iwochewitsch / François-Bernad Huyhe
connaissances personnelles et autres…