Espionnage industriel, Cybersécurité, cryptographie, ingénierie sociale, etc.

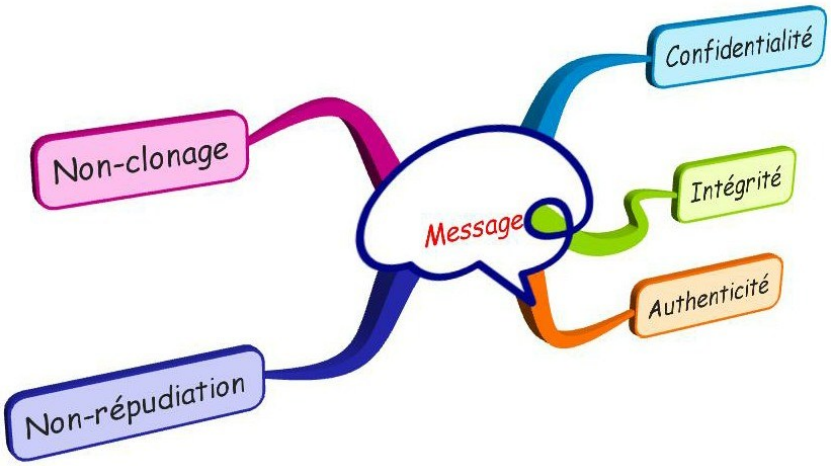
« Mieux vaut prévenir que guérir »

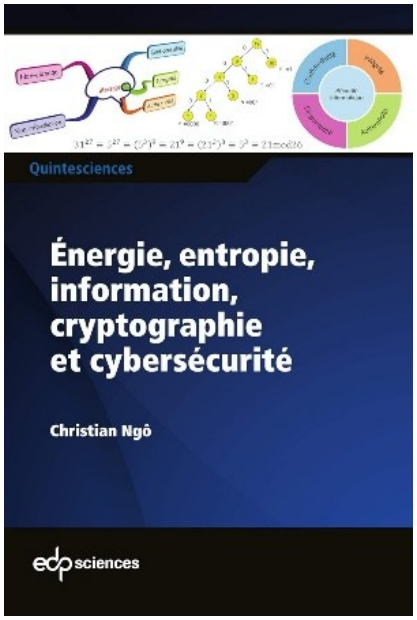
« Un homme averti en vaut deux »

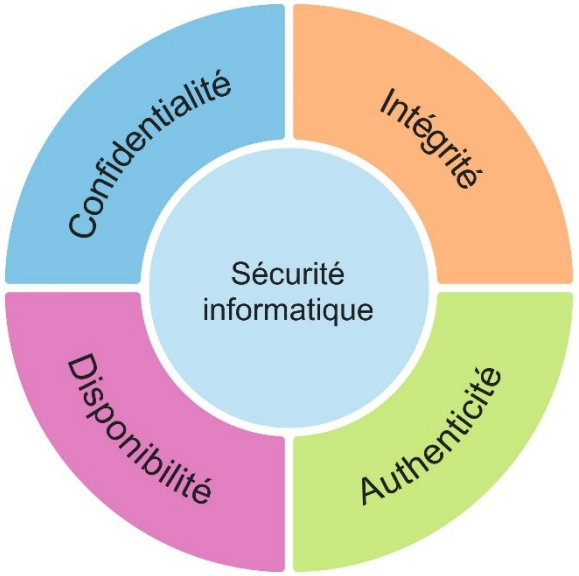
Christian Ngô

Edmonium

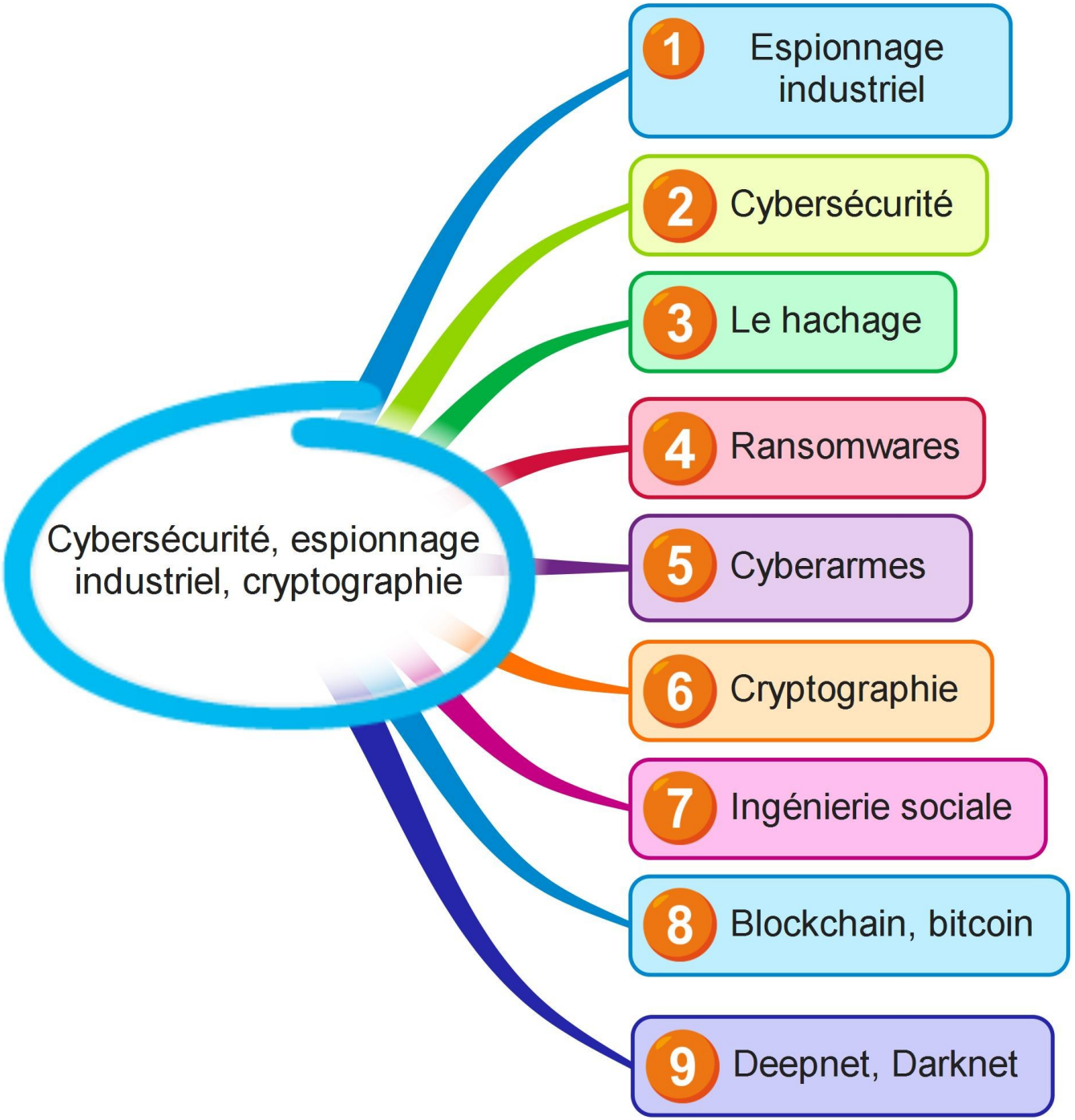
edmonium@gmail.com



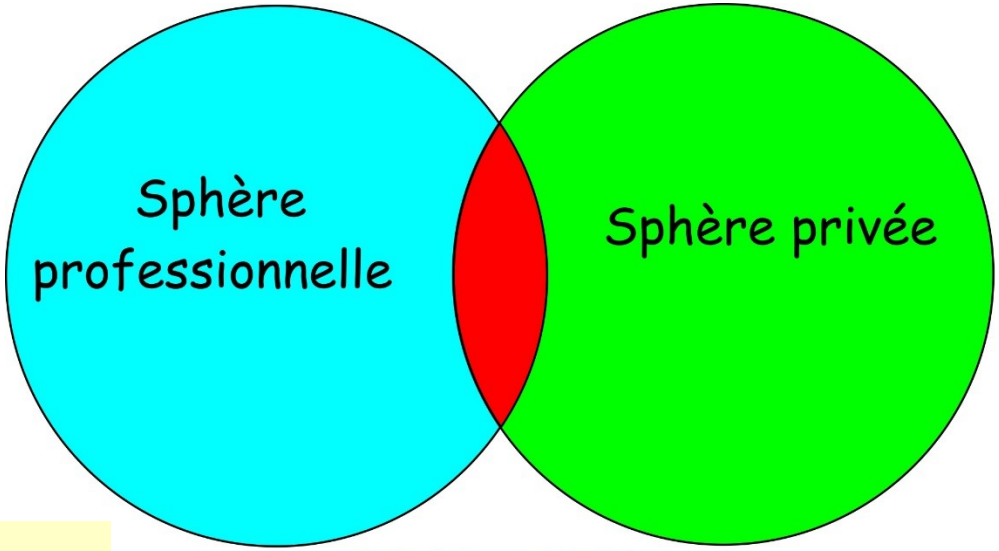




吳

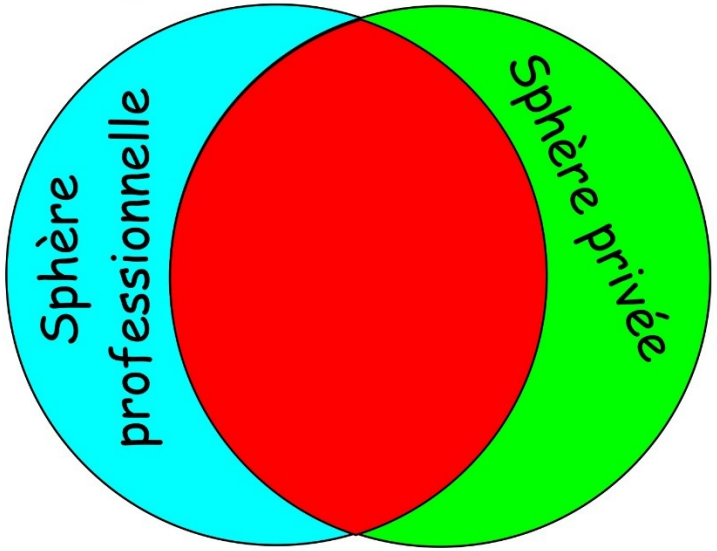

Cybersécurité, espionnage industriel, cryptographie
1 Espionnage industriel
2 Cybersécurité
3 Le hachage
4 Ransomwares
5 Cyberarmes
6 Cryptographie
7 Ingénierie sociale
8 Blockchain, bitcoin
9 Deepnet, Darknet

Vie privée et vie professionnelle sont de plus en plus liées



Avant

Les attaques d'une entreprise peuvent passer par la sphère privée



Aujourd'hui

1. Espionnage industriel

Espionnage industriel

Moyens illicites pour obtenir les secrets de ses concurrents

C'est tricher (au bridge : « un bon coup d'œil vaut mieux qu'une mauvaise impasse »)

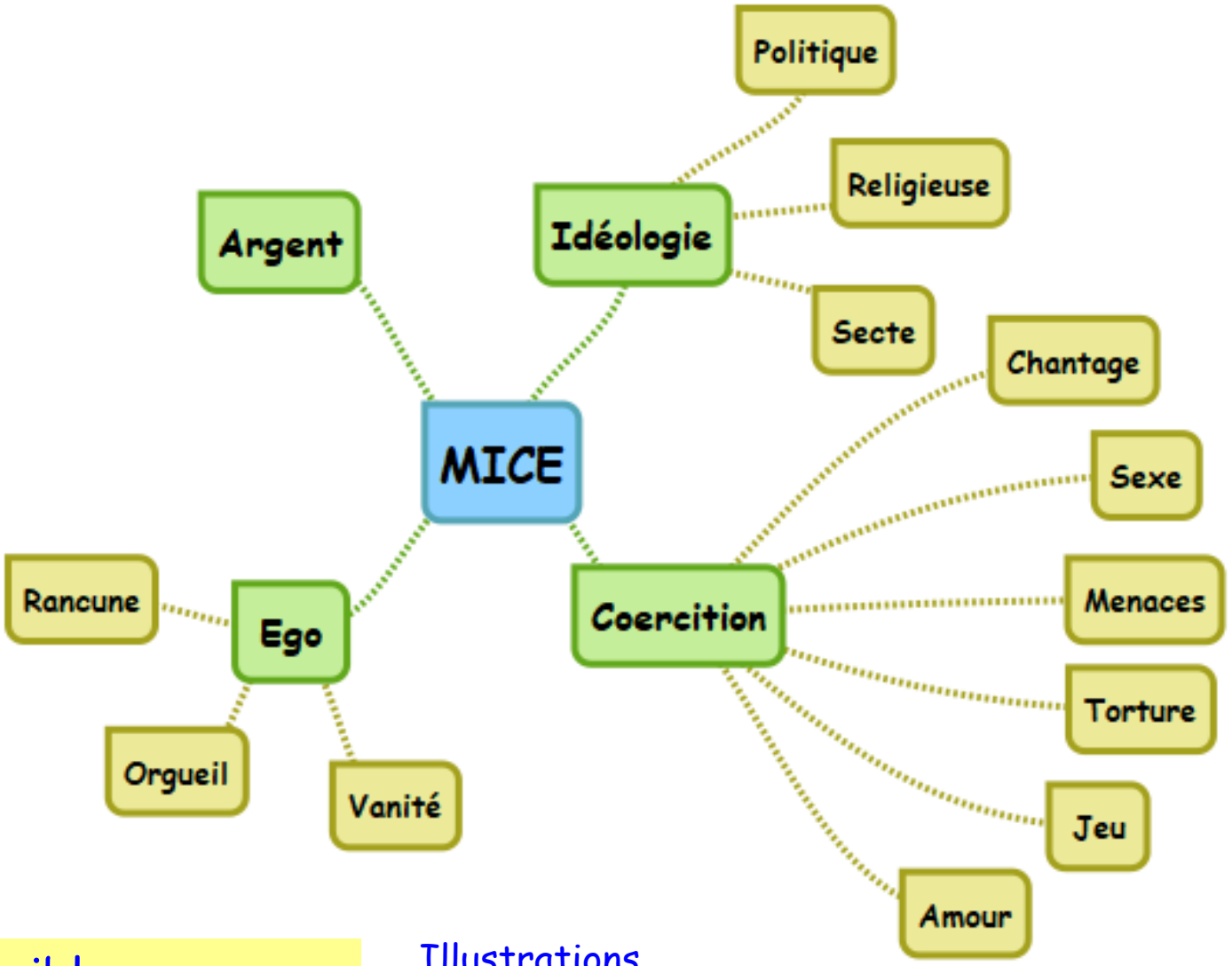
Reconversion des espions d'état en espions industriels

Exemples de risques :

- ❑ Voyages en avion ou en train
- ❑ Stagiaires
- ❑ Poubelles
- ❑ Ecoutes téléphoniques
- ❑ Copie disque dur à l'hôtel
- ❑ Manipulation de personnes
- ❑ etc.

Moyens de pression sur une personne

MICE ⇒
Money
Ideology
Coercition
Ego



Si vous êtes une cible une équipe projet s'occupe de vous

Illustrations
- ❑ Voyage touristique
- ❑ Espion qui s'est marié

L'espionnage industriel

https://www.youtube.com/watch?v=shEtY_sA_SM

2018

吳

Le cas du Concorde

https://www.youtube.com/watch?v=-3pah8atlug

2012

Guerre économique

Un exemple d'attaque réussie de nos « amis » : Alstom

- Utilisation d'outils militaires (NSA). Frédéric Pierucci : 2 ans de prison. 1 millions de mails piratés
- Utilisation de l'extraterritorialité : Contrat Indonésie-France qui ne plait pas aux USA et poursuites de leur part
- ITAR (International ,Traffic Arms Regulation) : 22000 produits ou composants
- American Patriot Act (2001) Toute entreprise française rachetée en totalité ou en partie par une entreprise américaine doit donner accès à toutes ses informations (perquisitions illégales)
- Récompense pour le dirigeant des entreprises achetées

呆

Edmonium

L'OSINT

Open Source INTelligence

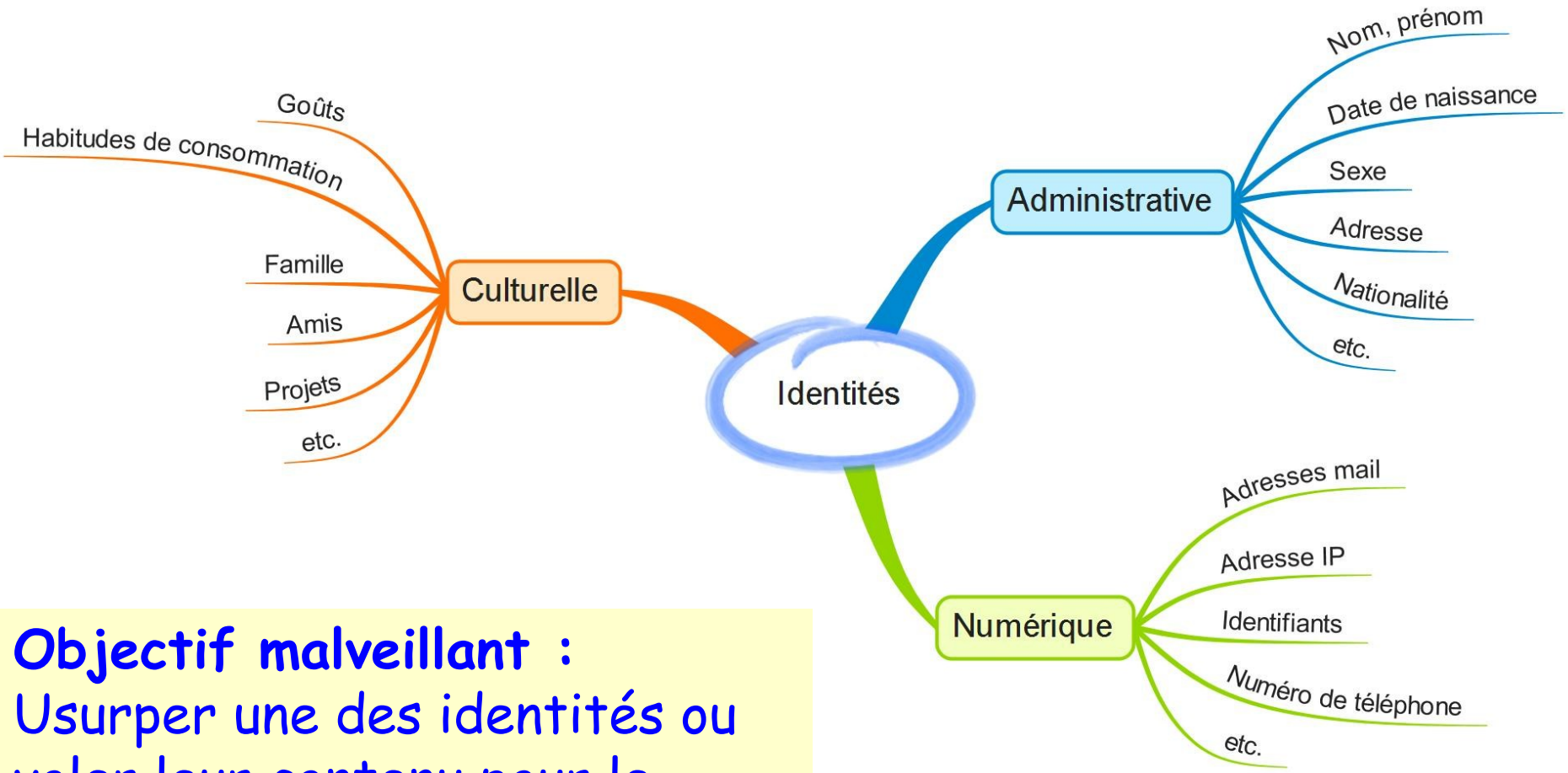
Méthode très efficace pour obtenir des informations à partir de sources ouvertes accessibles sur le net.

- OSD (Open Source Data). Données à l'état brut. Photo, compte rendu, etc.
- OSIF (Open Source Information). Données synthétisées dans un article, rapport, etc. (Attention aux fake news !)
- OSINT (Open Source INTelligence). Synthèse d'un grand nombre de sources sur un problème donné accessible à un nombre restreint de personnes. Application des méthodes du renseignement à des sources ouvertes
- OSINT-V (Validated OSINT). Produit par un professionnel du renseignement ou une source ouverte. Information considérée comme ayant un haut niveau de sécurité.

Voir vidéos à la fin

2. Cybersécurité

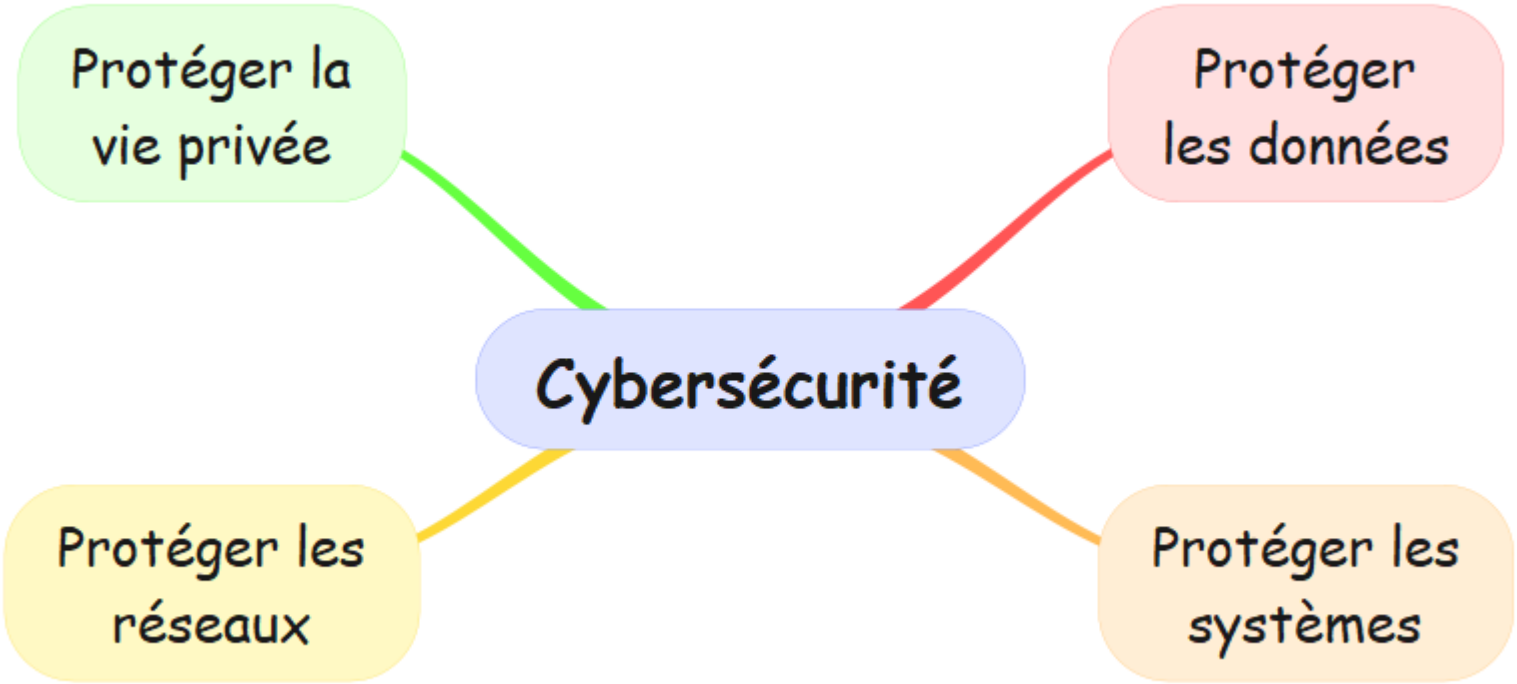
Vos différentes identités



Objectif malveillant :
Usurper une des identités ou voler leur contenu pour le revendre ou l'utiliser

Edmonium

Cybersécurité



Edmonium

Vulnérabilités

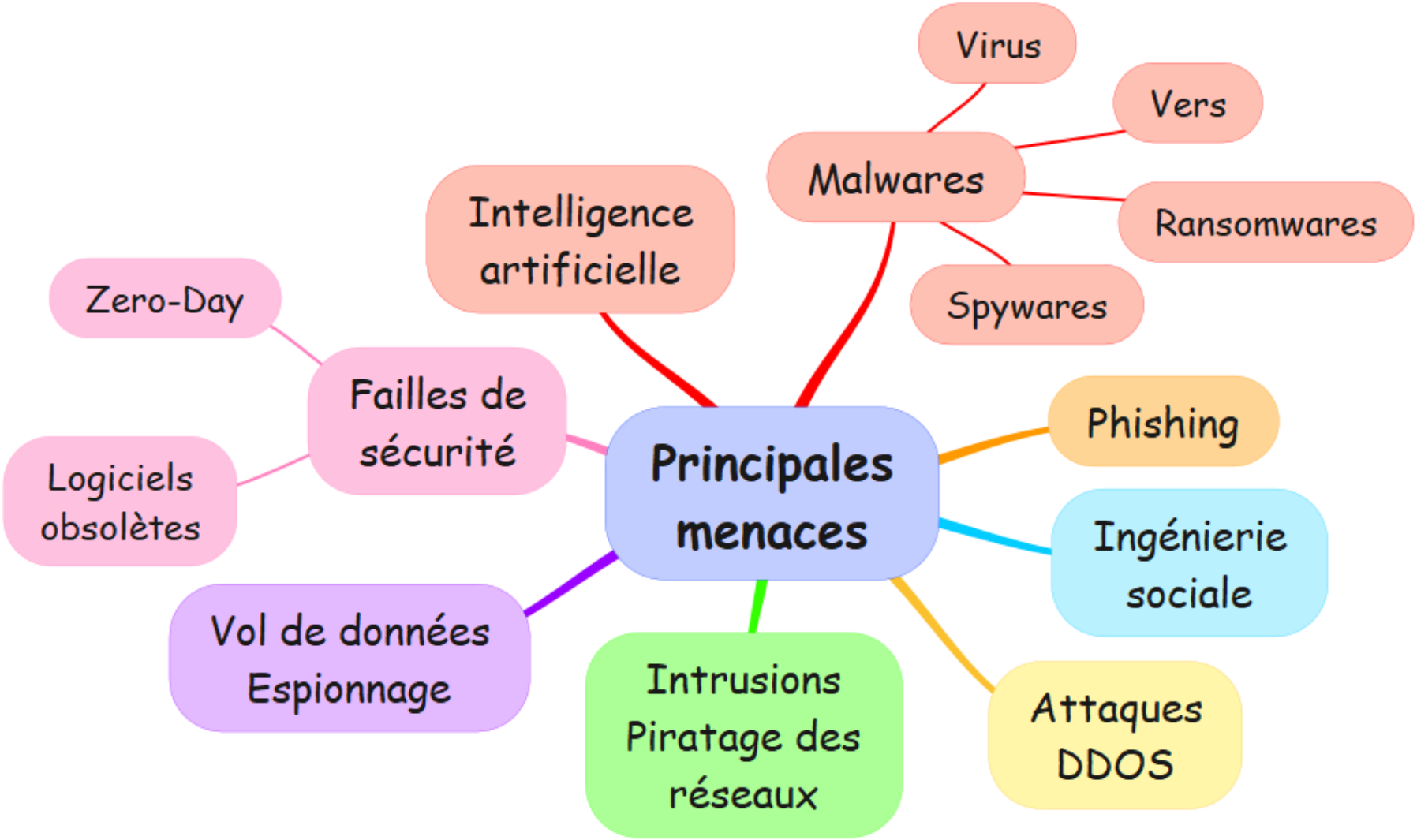
L'actif d'une entreprise comprend : les équipements matériels et logiciels, les brevets, les connaissances des processus, les fichiers clients, etc.
Ils ont tous une valeur pour l'entreprise

Vulnérabilités (vulnerability) ⇒ faille dans les actifs, les contrôles, les procédures
Menaces (threat) ⇒ exploiter une vulnérabilité
Contre-mesures ⇒ Elles servent à prévenir, détecter et réparer une attaque

Les systèmes d'information sont maintenant omniprésents. Ne pas savoir se servir d'un ordinateur est aujourd'hui un handicap

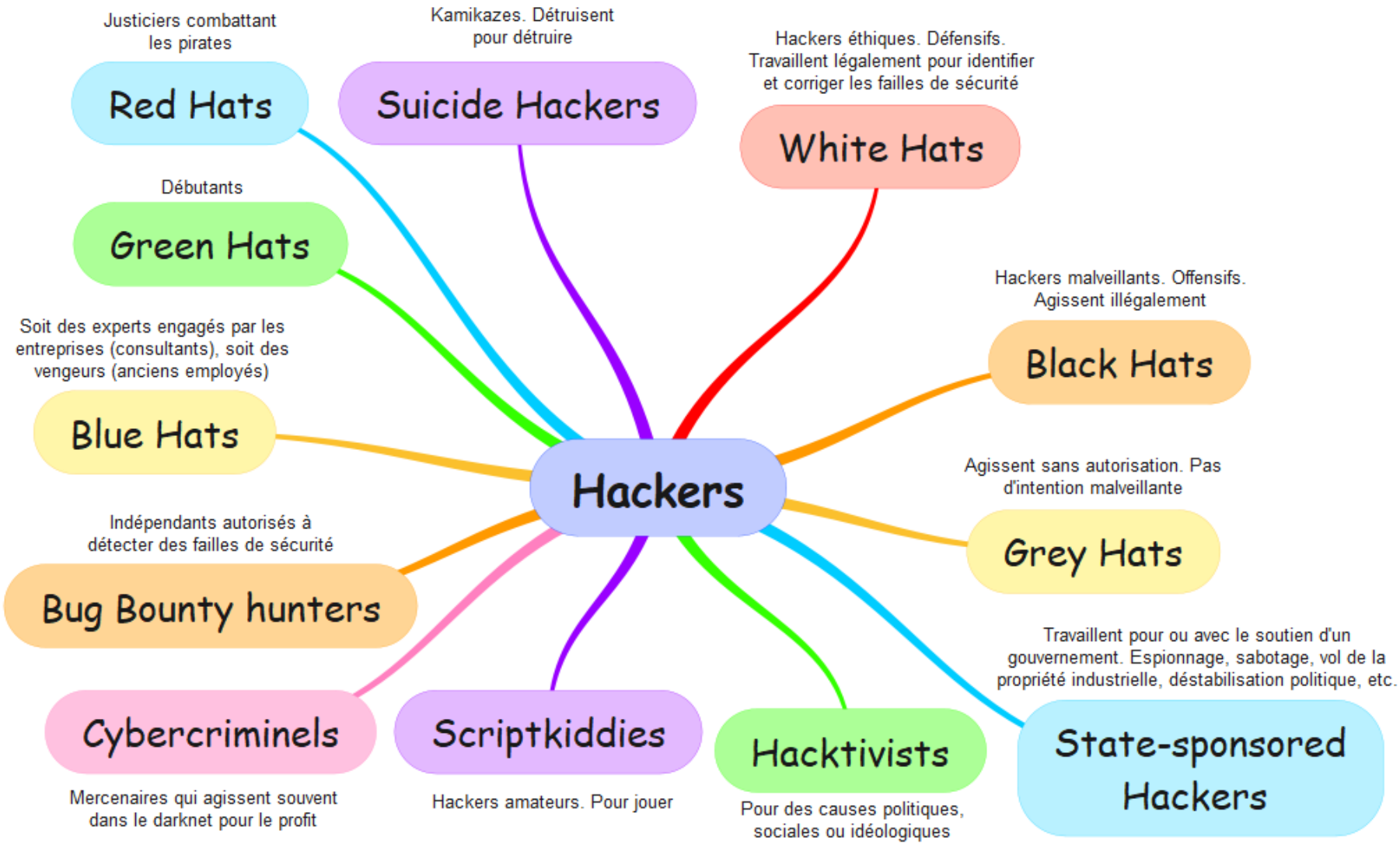
Edmonium

Menaces



Edmonium

Hackers (pirates)



Edmonium

Illustration : piratage d'aiguillages de tramway par un adolescent (2008)

- Janvier 2008 à Lodz (Pologne). Un adolescent de 14 ans fait dérailler un tramway qui en a percuté un second venant en sens inverse (12 blessés)
- Avant cet évènement : dysfonctionnements et déraillements
- L'adolescent avait transformé une télécommande IR pour la télévision et pouvait interagir le contrôle des aiguillages
- Il avait beaucoup appris en se promenant dans les dépôts de tramways et avait même fait un brillant exposé devant sa classe.
- Il avait ramené du matériel pour construire un système pouvant interagir avec le système de tramways
- C'était un élève modèle et un petit génie en électronique qui voulait juste faire une farce

Danger et risque

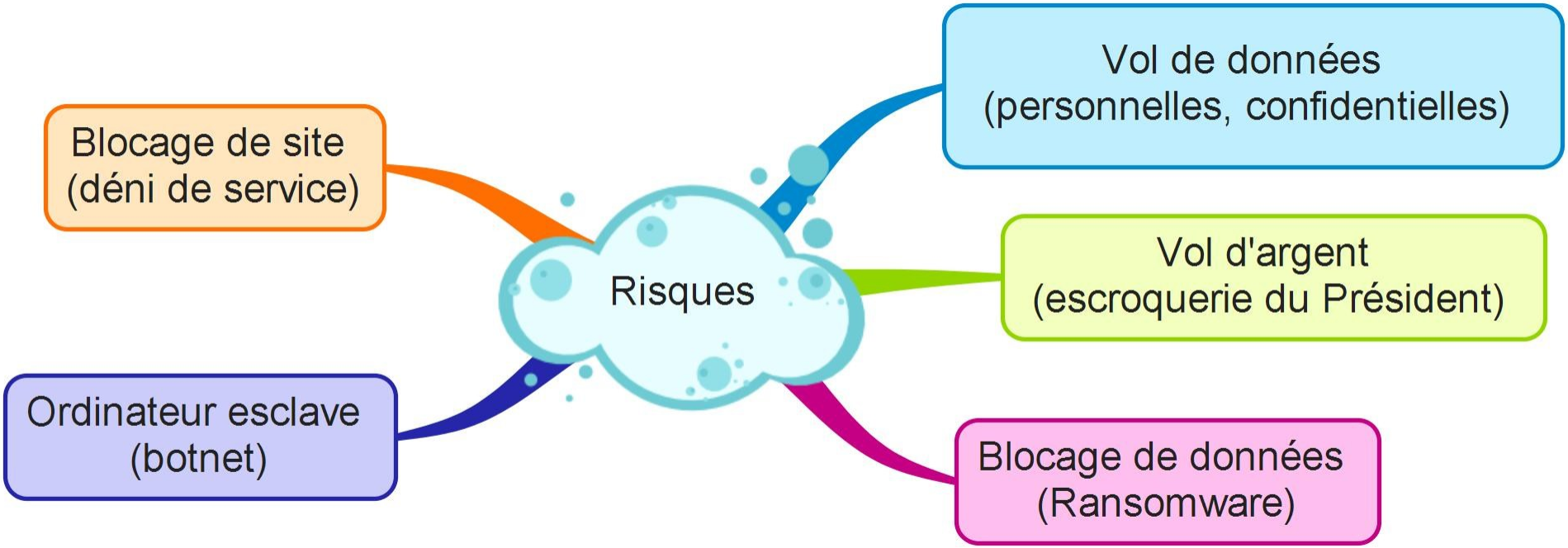
Danger ≠ Risque

Danger = Risque ⊗ Exposition

Quand on fait de l'escalade on risque de dévisser et de se tuer.
Mais si n'en fait pas il n'y a aucun danger de dévisser

Edmonium

Risques



Edmonium

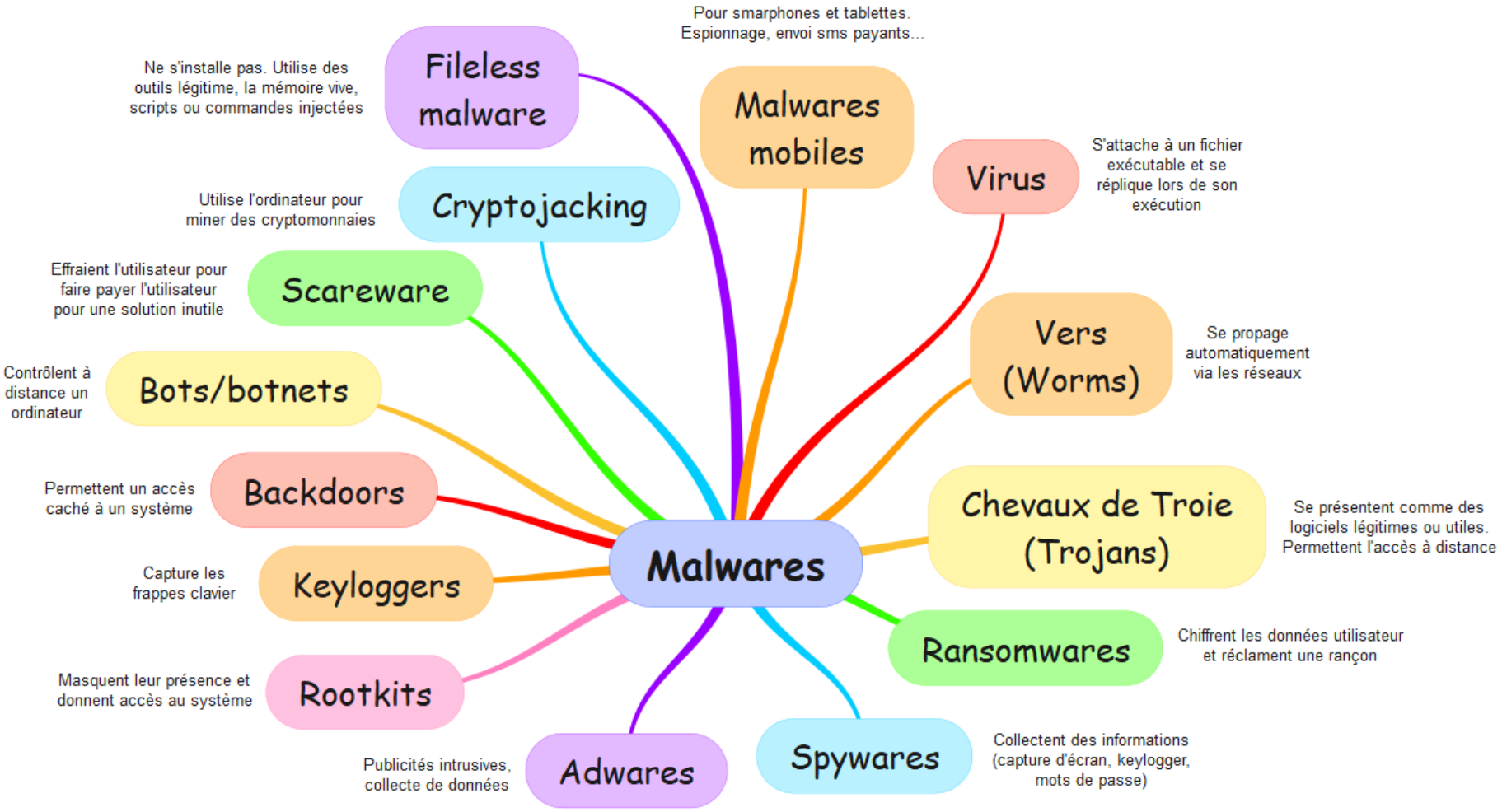
Malwares

Un malware est un logiciel malveillant permettant de compromettre un système informatique à l'insu de son propriétaire

Années 1970 : premiers malwares
Creeper ⇒ utilisait un modem et affichait : « I'm Creeper; catch me if you can ».
Depuis les malwares sont devenus beaucoup plus dangereux (exemple Stuxnet (centrifugeuses d'Iran) ou Flame en 2012)
Flame est resté en activité pendant des années sur des ordinateurs sans qu'on le sache. Il pouvait :
Collecter des informations, changer à distance les réglages, activer le micro, enregistrer des conversations, se connecter à des messageries instantanées, etc.
Il s'agit sans doute d'une cyberarme développée par un état.

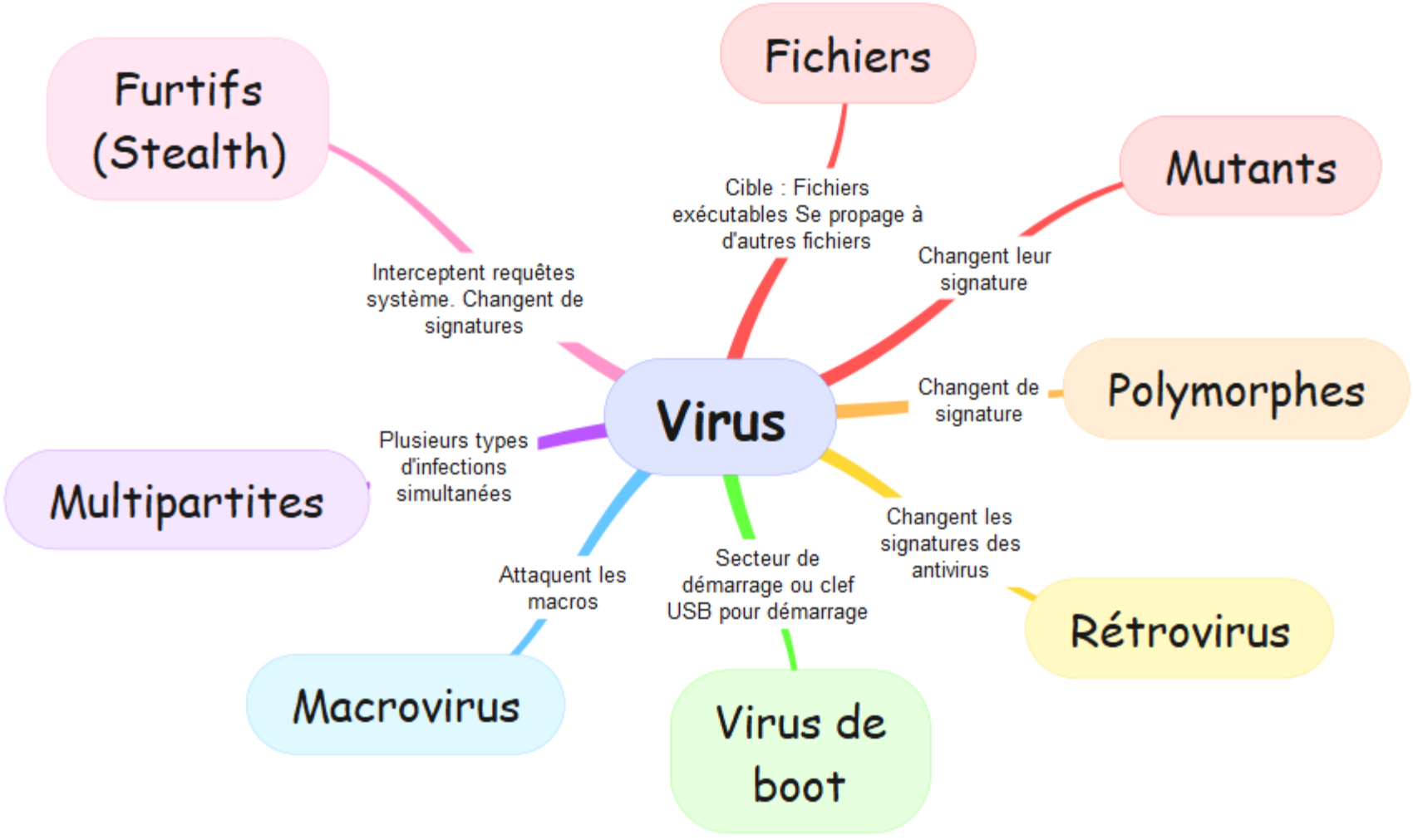
Edmonium

Malwares



Edmonium

Les virus



- Attaque zero day, exploit zero day
- Un antivirus ne détecte que les virus connus

吳

Edmonium

Attaque DOS et DDOS

DOS (Denial of service) DDOS (Distributed Denial of service)

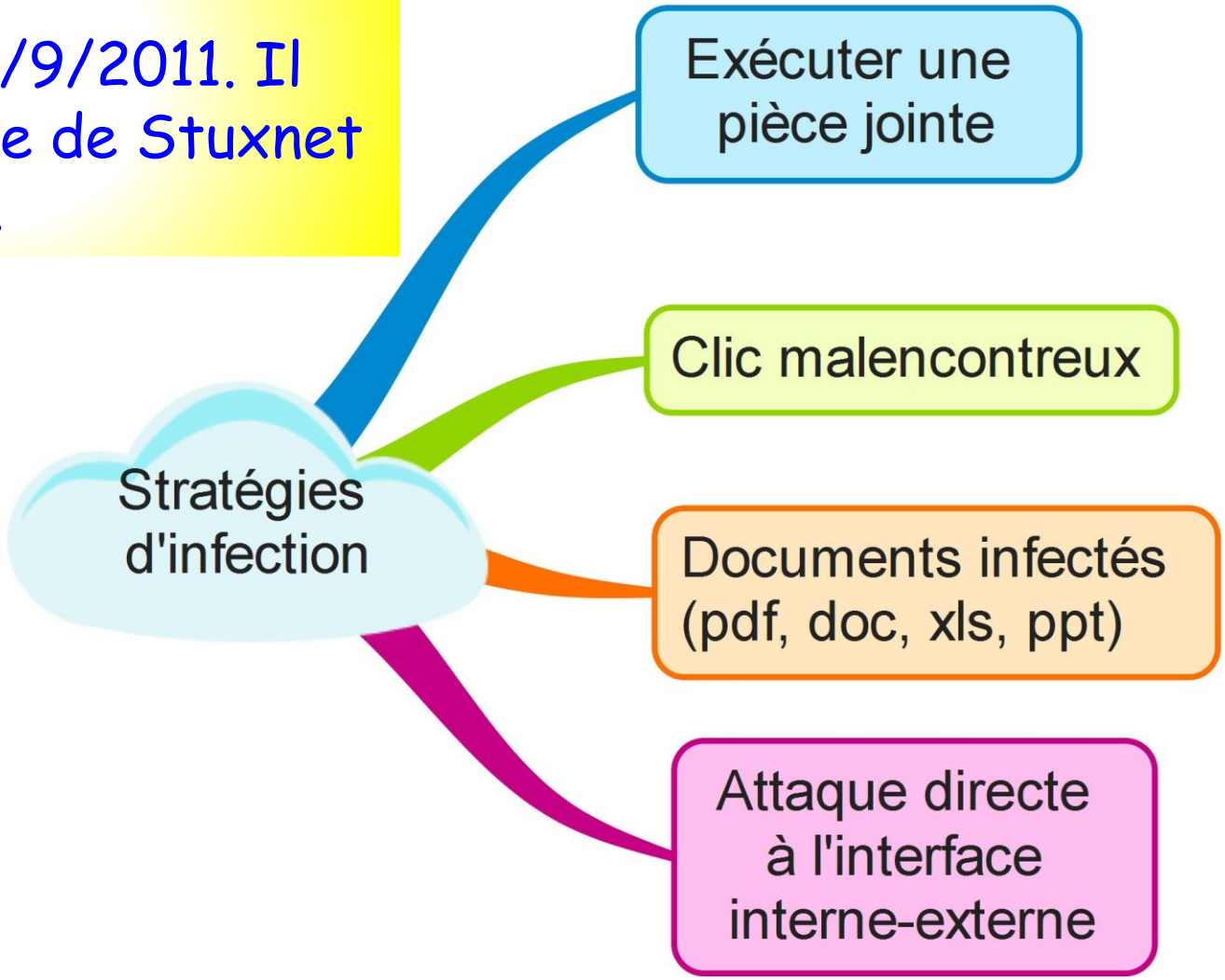
Envoyer des requêtes en continu pour que le système soit saturé et devienne indisponible pour les autres utilisateurs souhaitant se connecter.

On utilise pour cela un botnet composé d'ordinateurs et d'IOT (Internet Of Things, internet des objets)

Objectifs :
Gaming : ralentir l'adversaire
Sites gouvernementaux ou terroristes : pour des convictions idéologiques (ex: Anomymous, défense des libertés))
Entreprises : début d'une attaque de plus grande ampleur. Teste la capacité de réponse et diversion pour implémenter un malware

Stratégie d'infection

Exemple : Ver informatique Duqu
Découvert le 1/9/2011. Il est très proche de Stuxnet et sophistiqué.



Les attaques sont automatisées

Tout ordinateur connecté à internet ou à un réseau externe est susceptible d'être attaqué.

- Le pirate scrute réseau de manière aléatoire en envoyant des paquets de données.
- S'il voit un ordinateur connecté il cherche les failles

⇒ Il faut se protéger

- Antivirus
- Firewall (pare-feu). Fait respecter la politique de sécurité du réseau en contrôlant les paquets
- Proxy (pour protéger, rendre anonyme, jouer le rôle de cache)
- Zone démilitarisée (DMZ)

DeMilitarized Zone ⇒ sous réseau séparant le réseau local d'internet et protégé par un pare-feu. Les ordinateurs de la DMZ sont les seuls accessibles depuis internet

Edmonium

Le Proxy

https://www.youtube.com/watch?v=MpP02aZPSNQ

Qu'est-ce qu'un Bot ou un Botnet

https://www.youtube.com/watch?v=KnlU_t8wKPI

Les dégâts sur quelques exemples

- Le but des personnes qui utilisent les virus aujourd'hui est de gagner de l'argent (ex. ransomwares) ou, dans le cas d'une attaque faite par un État de perturber, détruire, contrôler des systèmes informatiques et des installations industrielles, financières, etc.
- 2007 : cyberattaque DDOS de l'Estonie (sites officiels, banques, médias…) : pays complètement déstabilisé
- 2008 Attaque DDOS de la Géorgie qui neutralisent toutes les infrastructures du pays.
- May 2011 Lockeed Martin paralysé pendant quelques heures et codes de sécurité volés
- 2017 (Wannacry, NotPetya, Adylkuzz). Sociétés touchées : Renault, Auchan, FedeX, Saint-Gobain, etc.
- Environ 180 000 cyberattaques/jour dans le monde

Spam

Mail non sollicité

- Spam publicitaire, Phishing, Scams, Forums et réseaux sociaux

- Le nombre de spam diminue (moins intéressant pour les spammeurs que d'autres techniques cybercriminelles) 60% de mails indésirables en 2015 contre 90% en 2010
- Démantèlement de botnets. Ex par Microsoft: botnet Waledac démantelé en 2010 (1,5 milliard de spams/jour). 2011 -> Rustock comprenait 1 million de botnets et avait généré 47% des spams mondiaux pendant 4 ans.
- En 2015 environ 8 spams/seconde au niveau mondial (50 spams/seconde début 2008)
- https://www.spamcop.net/spamgraph.shtml?spamstats

Edmonium

Spam ⇒ contremesures

- Ils sont difficiles à détecter
- Ne pas installer des logiciels dont on n'est pas sûr ou dont on sait qu'ils ont des spywares (ex : Babylon translator, Go!Zilla, Download accelerator, KaZaA, Cute FTP, etc.)
- La désinstallation d'un logiciel qui a installé un spyware ne désinstalle pas nécessairement celui-ci et peut conduire à des dysfonctionnements du système.
- Utiliser des antisywares soit en temps (réel) soit en les exécutant de temps en temps pour les gratuits.
- Ad-Ware, Malware byte's antimalware, Spybot Search&Destroy)
- Avoir un parefeu (firewall) personnel

吳

Edmoniu

Le phishing (hameçonnage ou filoutage)

Obtenir des renseignements personnels en vue d'une usurpation d'identité

Chronopost.fr <info.chronopost@rumbodentro.com>

À moi

Chronopost vous informe que l'envoi de votre colis est en cours d'achévement.

- Nous avons l'honneur de vous informer par le présent que nous avons reçu un colis volumineux qui a été envoyé par votre expéditeur ce matin au bureau de poste et prêt à être livré à votre adresse de résidence ou en point relais.

- Nous revenons vers vous afin de vous informer qu'il est préferable de confirmer l'envoi de votre colis avant qu'il soit retourné a votre expéditeur.

- Veuillez confirmer l'envoi à domicile ou en point relais en suivant la procédure ci-dessous :

1

Appelez le service de confirmation Trois fois de suite:

N°:08 99 700 640

2

Vous allez recevoir le code de confirmation durant le troisiéme appel téléphonique.

3

Envoyez le code de confirmation a l'adresse mail suivante:

chronopost_service@workmail.com

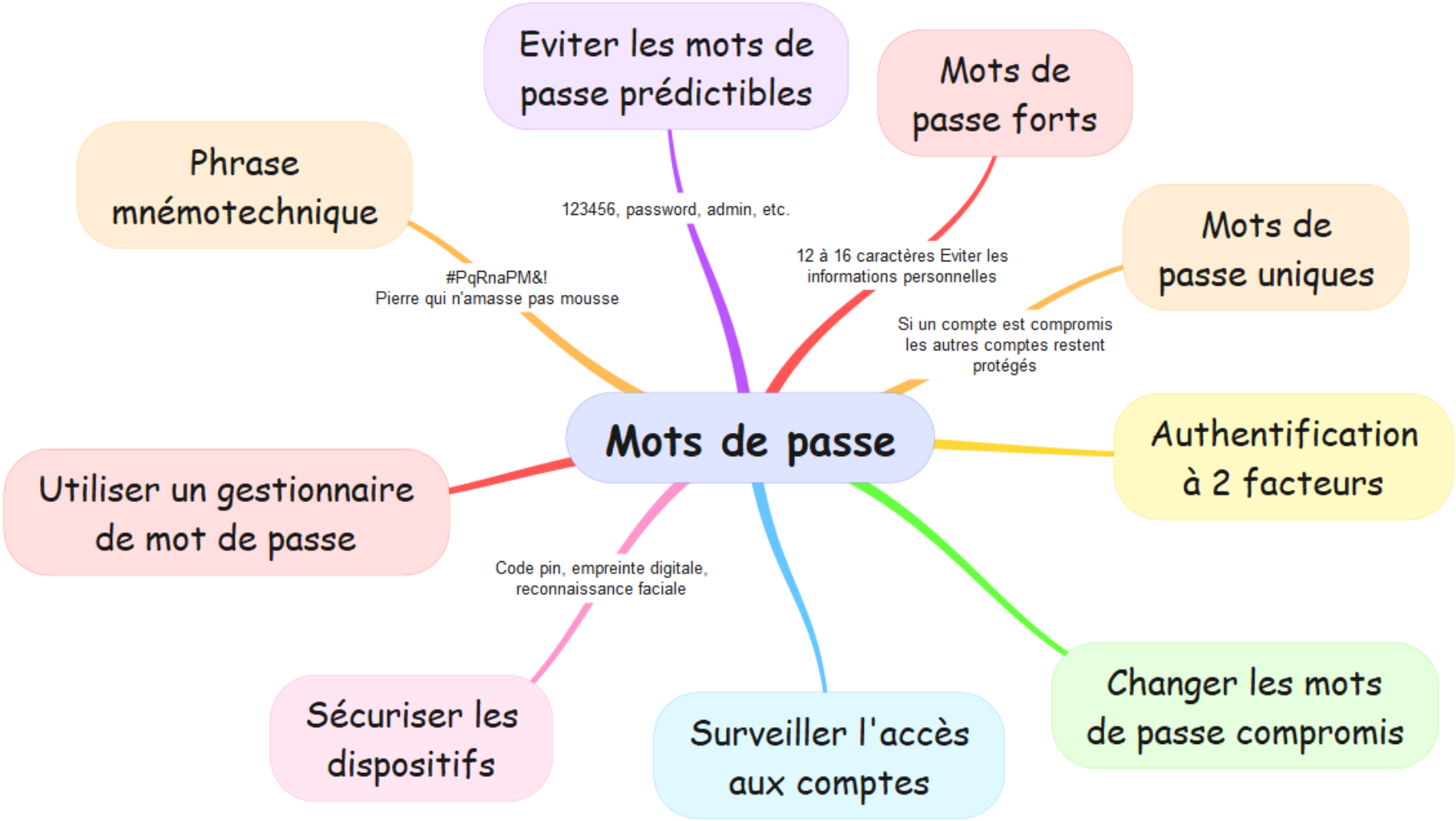
Edmonium

Cybersécurité

https://www.youtube.com/watch?v=hXyoRm1kkhE

Edmonium

Mots de passe



Ji32k7au4a83 est-il un bon mot de passe ?
Non car c'est my password tapé sur un clavier chinois

吳

Les Cookies

Petits programmes texte déposés dans votre ordinateur par le serveur sur lequel on est connecté.

- Permettent de gérer des sessions avec mot de passe lorsque l'internaute se reconnecte sur le même site
- Servent à pister l'utilisateur lors de ses recherches. Mouchard qui cherche à cerner le profil de l'internaute en vue de publicités ciblées

Gestion et contremesures

- Tous les accepter
- Tous les refuser (mais on ne peut accéder à certains sites)
- Naviguer incognito (navigation privée)
- Traiter individuellement les cookies

Edmonium

La fraude au clic

L'hébergeur d'une publicité est payé au clic.
Le coût pour l'annonceur dépend du nombre de clics

- L'hébergeur peut être tenté de cliquer sur la publicité
- Des entreprises concurrentes peuvent faire cliquer en masse par des humains ou des programmes automatiques
  ⇒ augmente le budget publicitaire du concurrent et si le budget journalier est limité fait disparaître l'annonce ce jour là (Adsense de Google).

La fraude pourrait représenter entre 10 et 30% des clics.

Edmonium

Effacer un fichier.

Pas si simple que ça

- Effacer un fichier c'est effacer son nom de la table des TOC (table of contents). Ce n'est pas effacer son contenu
- C'est comme enlever le nom d'une personne des pages d'un bottin
- Pour l'effacer il faut réécrire de manière aléatoire des 1 et des 0 une multitude fois sinon on peut le déchiffrer
- Avec des ssd ou des clefs USB on n'est pas sûr d'écrire à la même place. Mais déchiffrer demande des moyens importants
- Lorsqu'un disque dur, un ssd, une clef usb, etc. sont morts, il faut le démagnétiser et les détruire sinon il possible de récupérer les données ou une partie d'entre-elles. Voir par exemple : www.ontrack.fr

呆

Edmonium

Effacer un fichier.

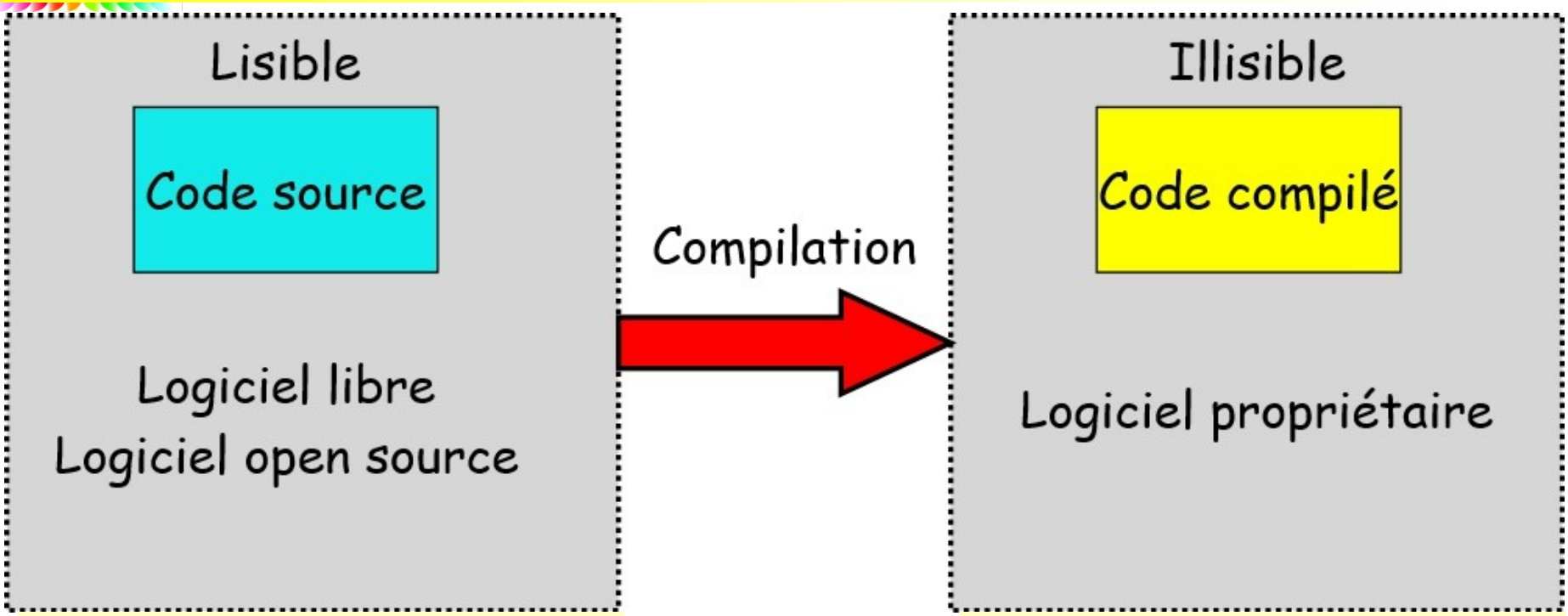
Pas si simple que ça

Principaux problèmes

- Avec les SSD, on n'écrit pas forcément au même endroit
- Avec les systèmes de fichiers intelligents comme sur NTFS, un journal garde la trace des modifications successives en cas de crash.
- Avec les systèmes à écriture redondante (comme RAID) il peut rester des traces ailleurs
- Effacer les traces d'un navigateur n'efface pas les fichiers
- Reformater un disque n'empêche pas de lire ce qui a été écris précédemment
- Pour ne laisser aucune trace ne travailler qu'en mémoire vive ou crypter

呆

Logiciels libres, open source, propriétaires



Ex: GNU/Linux, Libre office, etc.

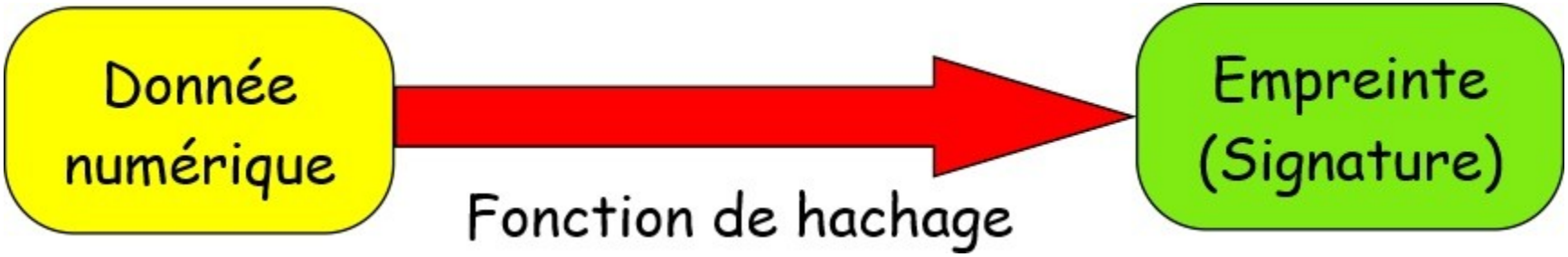
Ex: Windows, Mac OS, Microsoft office, etc.

Il existe une communauté.
Mieux contrôlé mais pas sûr à 100%
Attention aux extensions (firefox, chrome, etc.)

Fait-il seulement ce pourquoi il a été conçu ?
Ou backdoors, vol de données, etc.

3. Le hachage

Le hachage



- La longueur de la signature est toujours la même
- La signature (empreinte) est unique
- La fonction de hachage est une fonction à sens unique
- La probabilité de collision doit être extrêmement faible

Applications : mots de passe, téléchargement, etc.

Il existe plusieurs algorithmes

- MD5 (Message Digest 5 de Ronald Rivest, 1991)
- SHA1 (NSA) signature à 160 bits
- SHA2 (NSA) comprends SHA-224, SHA-256 et SHA-512

Edmonium

Le hachage

« Nous partîmes cinq cents ; mais par un prompt renfort – Nous nous vîmes trois mille en arrivant au port. »

Un hash 256 de cette phrase (http://www.convertstring.com/fr/Hash/SHA256) est :

2A9F932B44E7D2D5F60751948A35D9593D5257D0B6D62840
E117E32E2066A5D8

Prenons la même phrase, dans laquelle nous avons juste enlevé le point final.

« Nous partîmes cinq cents ; mais par un prompt renfort – Nous nous vîmes trois mille en arrivant au port »

Le même hash devient :

9FAE560ACDE202CDC3ECCEC86A93E3E974D23D0D29B-
C768ECAC389111DE8DF13

吳

Le hachage

https://www.youtube.com/watch?v=rO5aQzgKOs0&t=184s

Edmonium

4. Ransomwares

吳

Edmonium

Wannacry

2017

https://www.youtube.com/watch?v=aOS9-787lxY

吳

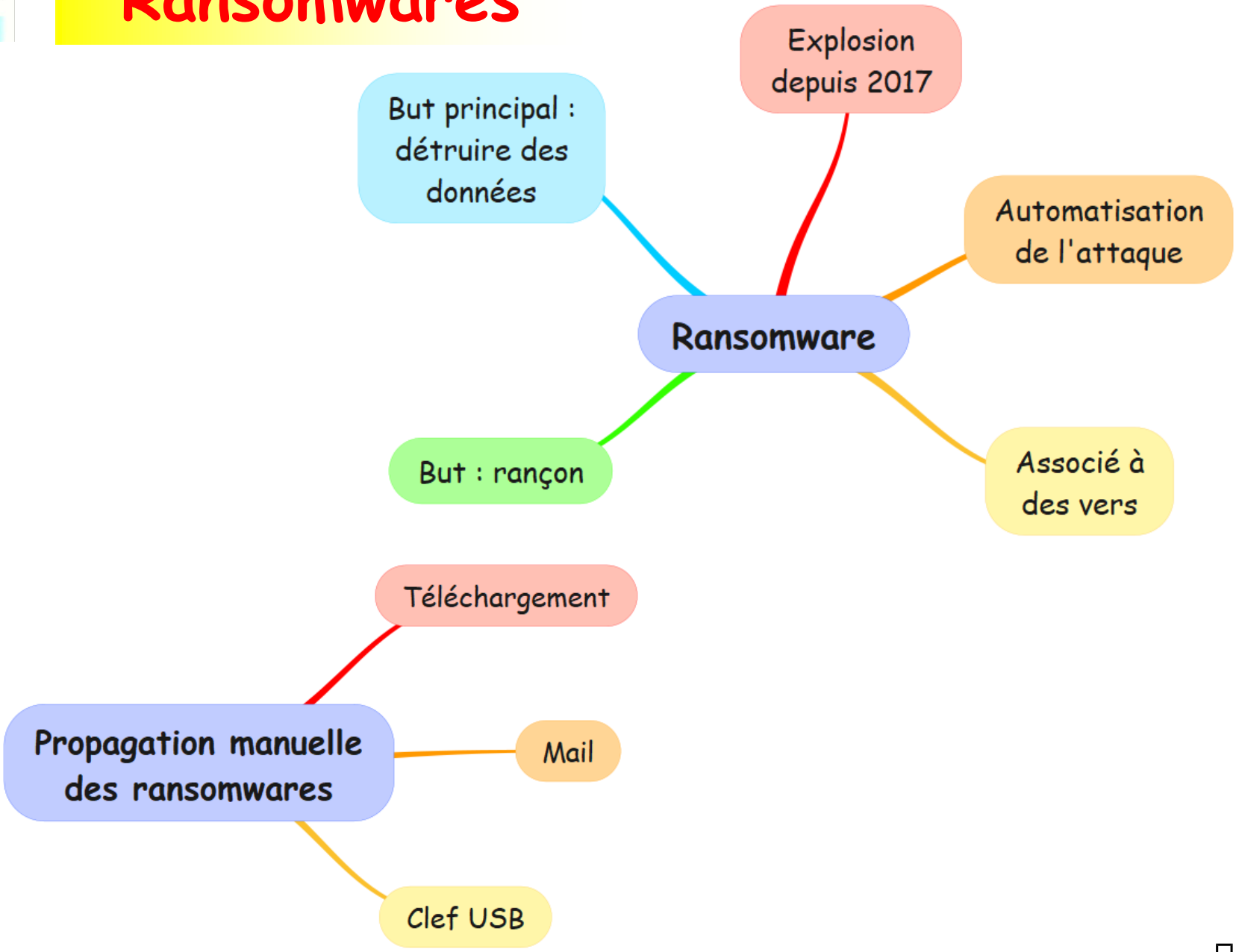
Edmonium

Les ransomwares ou rançongiciels

- Crypter les fichiers d'un ordinateur, en empêcher l'accès ou verrouiller le système d'exploitation
- Demande de rançon pour décrypter ou déverrouiller
- Ne pas payer car on n'est pas sûr qu'on aura la clef de déverrouillage en retour
- Se cache dans les mails, les pièces jointes, les macros de Microsoft office…
- Wannacry (mai 2017) a touché 300 000 ordinateurs et 150 pays. St Gobain : perte de 250 M€ (1% du CA). A utilisé un Web Exploit développé par la NSA (EternalBlue) et volé par les Shadow Brokers. Nombreuses sociétés touchées. Grosses pertes financières
- NotPetya (23 juin 2017). Destructeur de données mais aussi ransomware. L'entreprise de transport danoise Maersk a perdu 300 millions de $

Edmonium

Ransomwares



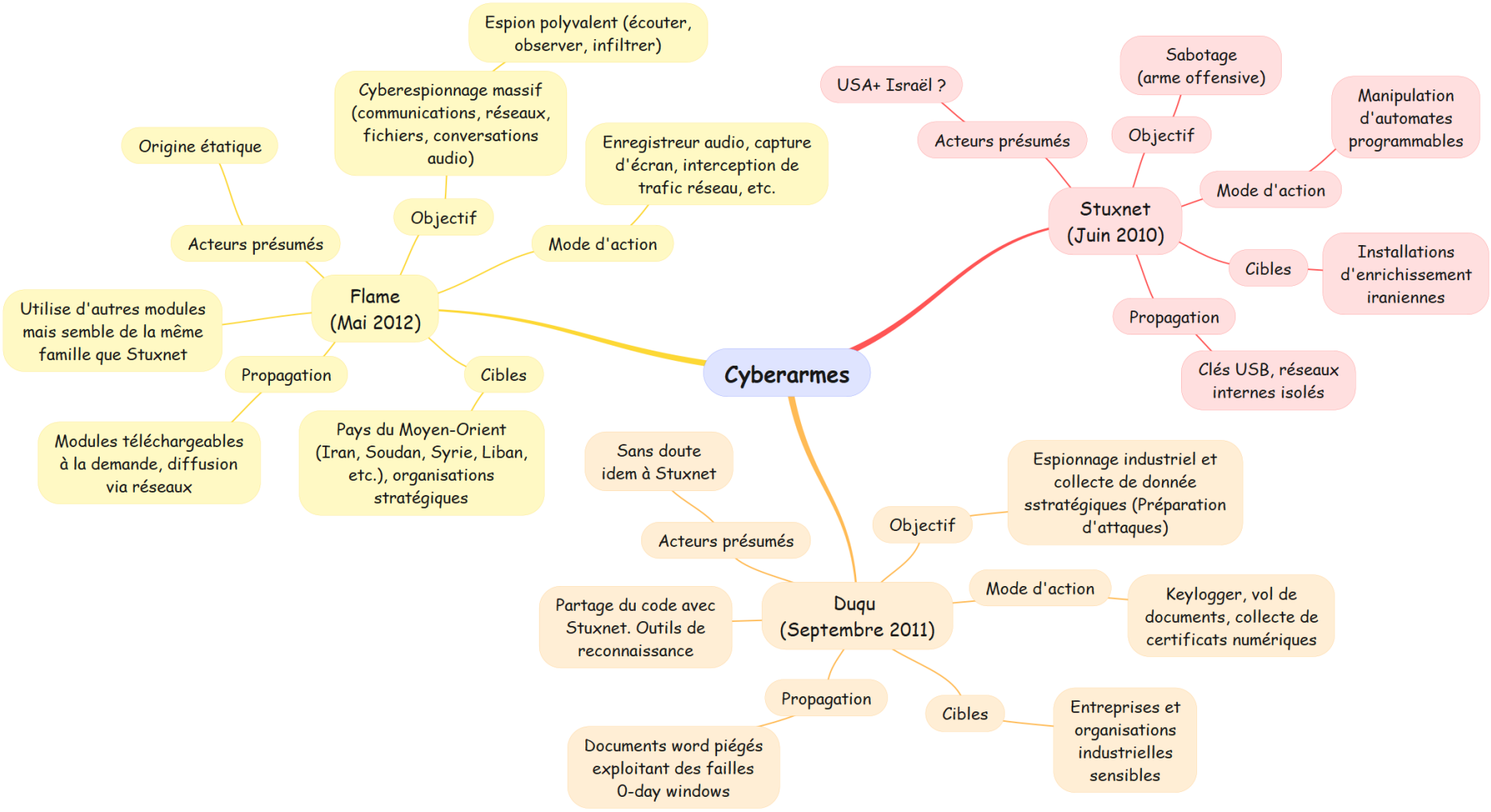
Edmonium

5. Cyberarmes

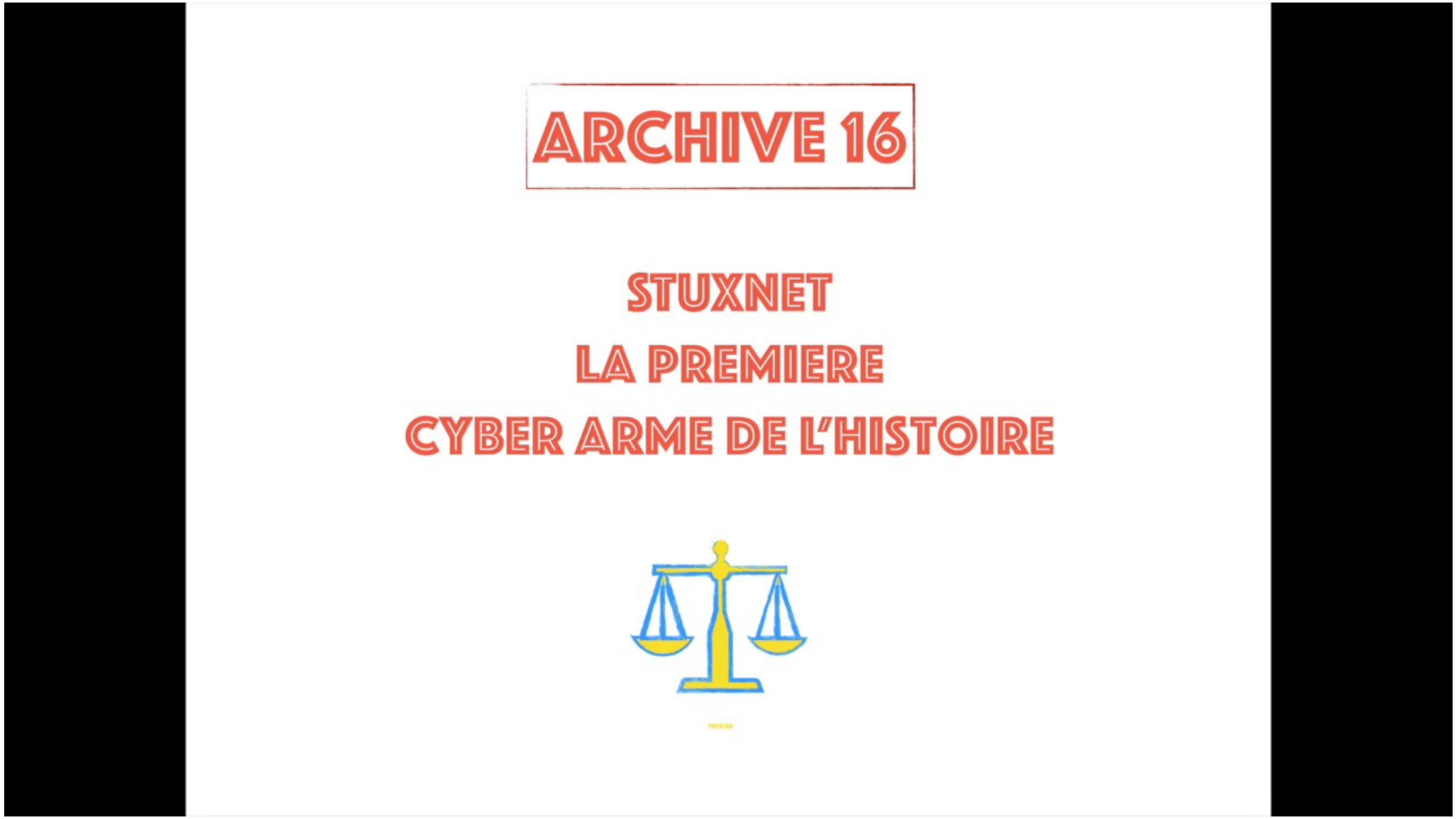
吳

Edmonium

Cyberarmes



La cyberarme Stuxnet



https://www.youtube.com/watch?v=Tk9eiXhIqT0

Edmonium

6. Cryptographie

吳

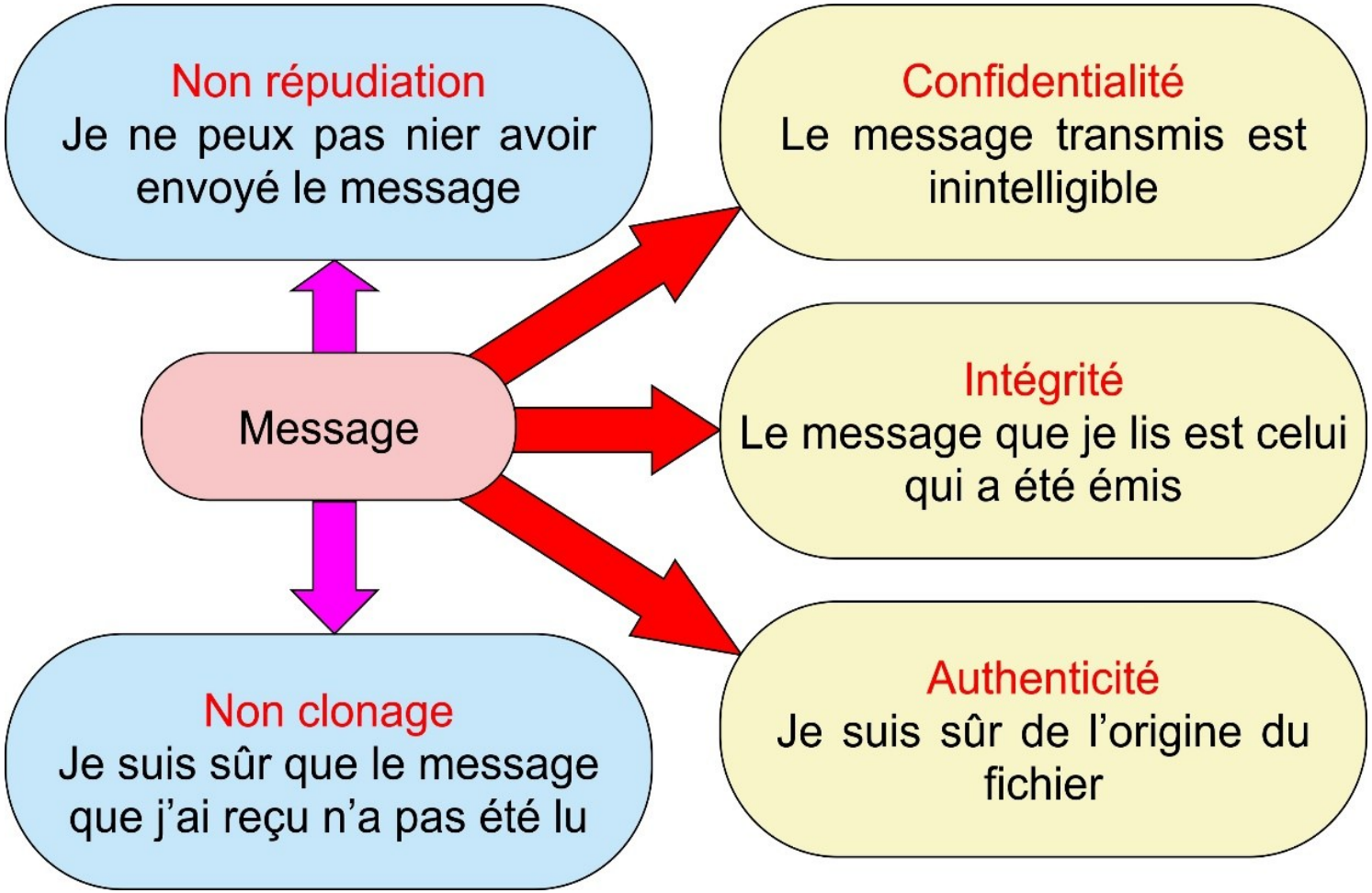
Cryptologie

Transmettre un message ne suffit pas : il faut protéger son contenu
Exemple dans l'antiquité chez les Grecs : écriture d'un msg sur le crâne d'un homme rasé et envoi du messager lorsque les cheveux avaient repoussé

Cryptologie = Cryptographie + cryptanalyse

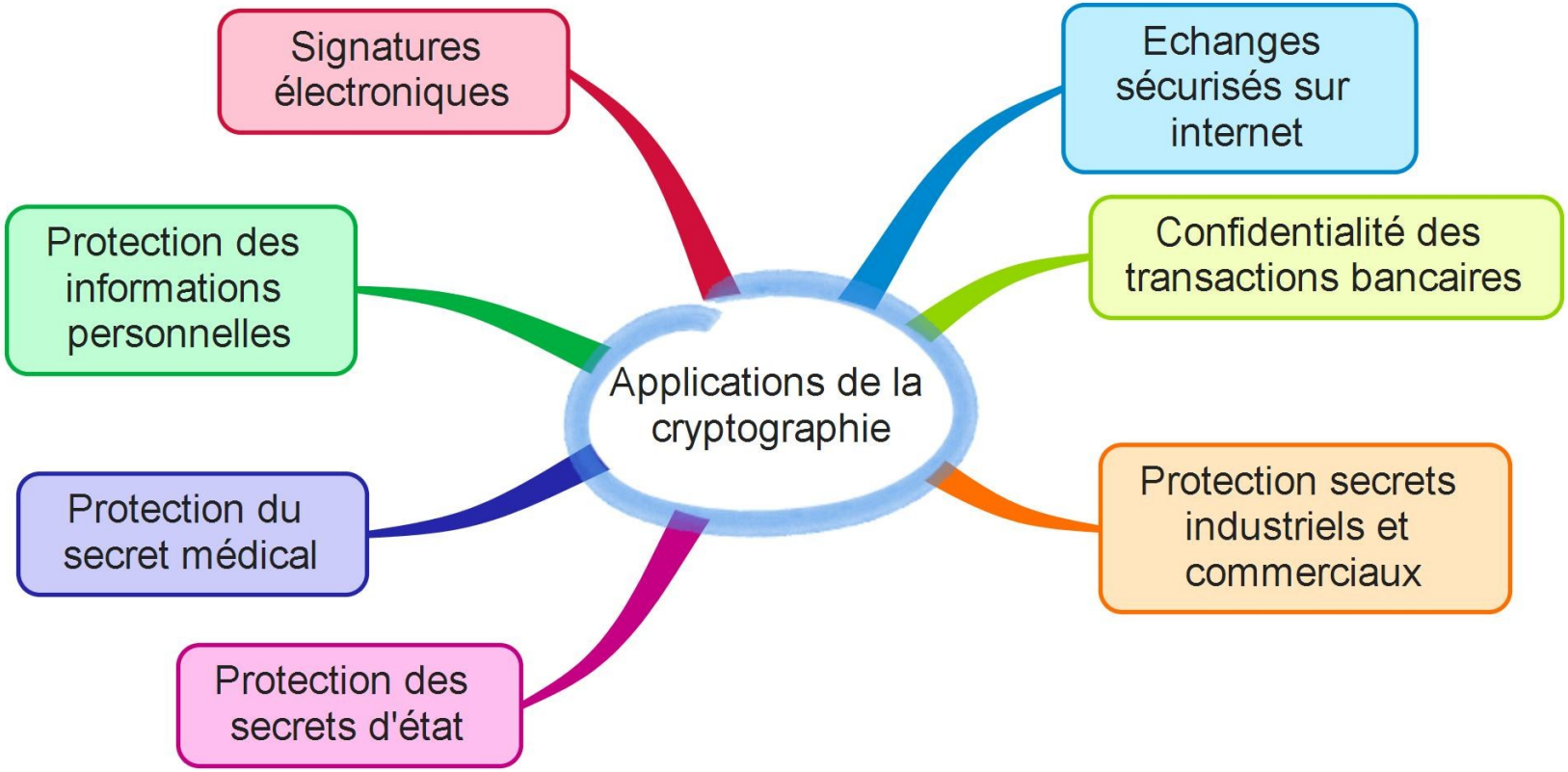
Cryptographie : art de cacher un message pour ceux qui ne sont pas destinés à en prendre connaissance.
Préserver la confidentialité de l'information et son intégrité
Cryptanalyse : art de trouver des attaques permettant de casser les protections mises en place par la crytographie.

Cryptographie



- ✓ L'émetteur peut prouver qu'il a écrit le message
- ✓ Le receveur ne peut nier l'avoir reçu
- ✓ L'émetteur peut prouver qu'il a envoyé le message

Cryptographie



Cryptographie

- Elle a longtemps été réservée aux militaires et diplomates
- En France elle a été considérée comme une arme de guerre. Il a été interdit de l'utiliser jusqu'en 1998
- Après 1998 on pouvait utiliser une clef de taille inférieure à 128 bits sans déclaration
- Depuis 2004 (loi du 21 juin pour la confiance dans l'économie numérique) la crytographie est autorisée mais une déclaration et une autorisation sont nécessaire pour l'importation ou exportation. Sans cette loi, l'économie numérique serait impossible en France

Auguste Kerckhoffs (la cryptographie militaire, 1883) a été le précurseur de la cryptographie moderne.
Pour lui la sécurité ne devait pas reposer sur la méthode cryptographique

Edmonium

Règles de Kerckhoffs

1. Le système doit être matériellement ou mathématiquement indéchiffrable
2. Il ne doit pas exiger de secret et peut tomber entre les mains de l'ennemi.
3. La clef doit pouvoir être retenue facilement
4. Il faut qu'il soit applicable à la correspondance télégraphique
5. Il doit être portatif et ne pas nécessiter plusieurs personnes pour le mettre en œuvre
6. Le système doit être facile à utiliser.

呆

Edmonium

Règles de Kerckhoffs pour le contexte d'aujourd'hui

1. La sécurité du système cryptographique doit reposer sur le secret de la clef et non sur celui de l'algorithme.
2. Le déchiffrement sans la clef doit être impossible avec les moyens du moment car nécessitant des temps astronomiques.
3. Si l'on connaît le message en clair et sa version cryptée, il ne doit pas être possible d'en extraire la clef en un temps raisonnable.

Il vaut mieux un algorithme public que propriétaire
Exemple : les chiffrements propriétaire des GSM (A5/0 et A5/1) et des DVD (CSS) ont été cassés en quelques semaines.

吳

Edmonium

Congruence

Soient deux nombres entiers a, b et un nombre entier $n \geq 2$.

a est congru à b modulo n si n divise la différence $b - a$

$$a \equiv b \bmod n$$

On peut définir l'addition et la multiplication dans $Z/\!/nZ$

exemples dans $Z/\!/26Z$

Si $n = 26$ on a $31 \equiv 5 \bmod 26$

On a aussi $157 \equiv 1 \bmod 26$

$-2 \equiv 24 \bmod 26$

$Z\equiv$ ensemble des nombres relatifs

$Z/\!/nZ\equiv$ ensemble des éléments de Z modulo n

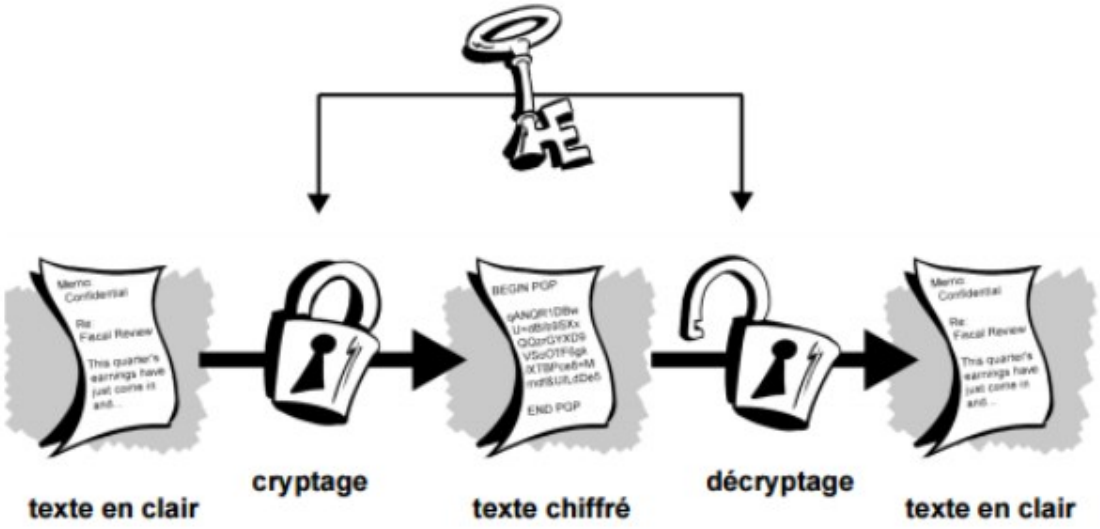
$Z/\!/nZ$ contient n éléments

$\forall a \in Z= \Rightarrow \quad a = dn + r$

On a donc $a \equiv r \bmod n$ et $0 \leq r < n$

吳

Chiffrement symétrique



- ✓ En pratique la clé de chiffrement est identique à celle de déchiffrement.
- ✓ Le danger se situe au niveau du transfert de la clé
- ✓ Les systèmes par flots (stream ciphers) opèrent sur les caractères, les systèmes par block (block ciphers) opèrent sur des mots (blocs)
- ✓ Exemple : DES (Data Encryption Standard, 1975)

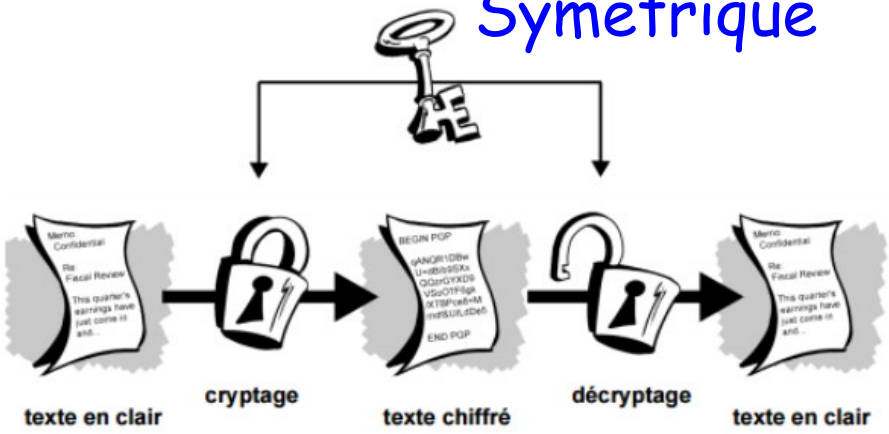
Historique au 20ème siècle

1919-1975
Cryptage symétrique

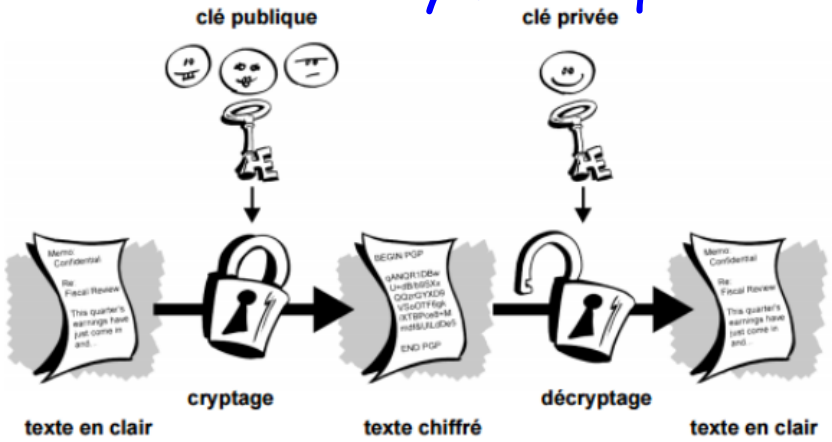
À partir de 1976
- ✓ Cryptographie à clé publique (asymétrique)
- ✓ Une clé publique connue de tous
- ✓ Seule la clé de déchiffrement reste secrète

1978 premier système de chiffrement à clé publique (RSA) qui peut résister à la cryptanalyse

Symétrique



Asymétrique



RSA = Rivest Shamir Adleman

Edmonium

Complexité

Beaucoup des algorithmes de cryptographie sont basés sur la multiplication de nombres premiers et la factorisation

- 127+457=584 $\Rightarrow$ environ 3 opérations + retenues. Pour n chiffres, complexité $\approx n$
- 127×457=58 039$\Rightarrow$ 9 opérations + retenues. Complexité varie comme $\approx n^2$
- Pour factoriser 58 039, la complexité varie comme $\exp(4n^{1/3})$
- Si on prend des nombres premiers de 200 chiffres, n^2=40 000 (multiplication) mais la complexité pour la factorisation est de 14 423 748 777 soit 360 593 fois plus
- Calculer le produit de deux nombres premiers p et q (pq) se calcule beaucoup plus facilement que de factoriser le produit pq. C'est le principe de la cryptographie asymétrique

Edmonium

Fonction à sens unique, fonction trappe

Une fonction bijective $f(x)$ est dite à sens unique si on peut facilement calculer $f(x)$ à partir de x mais si le calcul inverse est extrêmement difficile

En cryptographie, cela veut dire que chiffrer (f) est rapide mais déchiffrer (f^{-1}) demande un temps extrêmement long.

On ne peut donc pas utiliser f^{-1} pour déchiffrer. On utilise une fonction trappe qui appartient à une famille de fonctions à sens unique f_t dépendant d'un indice t qui permet de rapidement calculer f_t si on connaît t

吳

Fonction à sens unique, fonction trappe

Soit $f : x \mapsto x^3 \pmod{100}$. On veut trouver x tel que $x^3 \equiv 11 \pmod{100}$

Il faut tester tous les nombres de 0 à 99 pour trouver le bon.

On trouvera 71. En effet $71^3 = 357911 \equiv 11 \pmod{100}$

Il existe une fonction trappe qui permet d'obtenir facilement le résultat. C'est $f : y \mapsto y^7 \pmod{100}$

On opère de la façon suivante :

On prend pour y le résultat congru que l'on cherche (ici 11)

$11^7 = 19487171 \equiv 71 \pmod{100}$

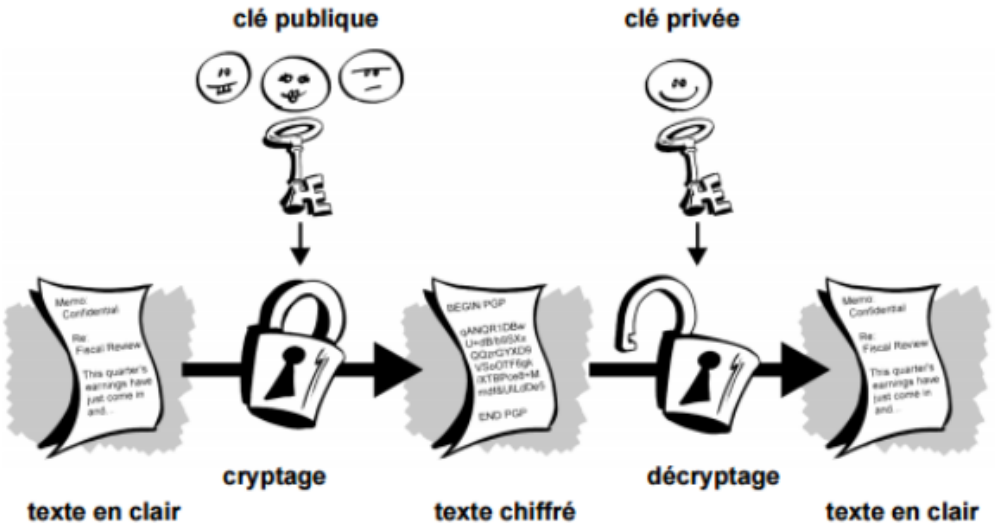
On peut vérifier sur une autre valeur

Si $x^3 \equiv 23 \pmod{100}$

$23^7 = 3404825447 \equiv 47 \pmod{100}$ et l'on peut vérifier que

$47^3 \equiv 23 \pmod{100}$

Chiffrement asymétrique



- ✓ La clé de chiffrement est publique, la clé de déchiffrement est privée.
- ✓ Analogie avec une boite aux lettres
- ✓ Introduit en 1976 par Whitfield Diffie et Martin Hellman d'une part et Ralph Merkle
- ✓ Inconvénient 100 à 1000 fois plus lent que le chiffrement symétrique
- ✓ Exemple : protocole SSL (Secure Sockets Layers)

Code RSA

Clef publique accessible à tous. Clef privée accessible seulement à celui qui doit décoder le message

Bob veut envoyer un message à Alice

- Alice génère 2 clefs : une clef publique et une clef privée pour son usage personnel
- Bob crypte son message avec la clef publique d'Alice et l'envoie à Alice
- Alice utilise sa clef privée pour décoder le message de Bob

Génération des clefs

On prend deux nombres premiers distincts p et q

$n = p \times q$ (module de chiffrement) et $\varphi(n) = (p-1) \times (q-1)$

On choisit un exposant e qui soit premier avec $\varphi(n)$

et on calcule d l'inverse de $e \bmod(\varphi(n))$

La clef publique est le couple (n, e)

La clef privée est d

Code RSA

Chiffrement

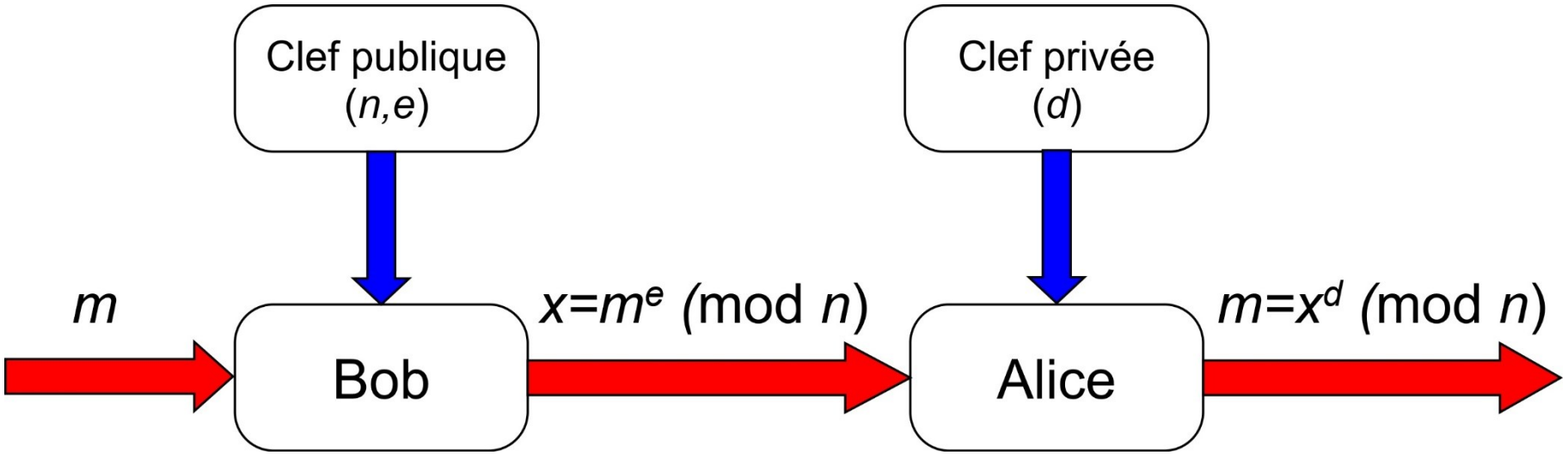
Bob convertit son message en chiffres.
Cela génère un ou plusieurs entiers m
Le message chiffré est calculé par la formule

$$x = m^e \pmod{n}$$

Déchiffrement

Alice reçoit x
Elle utilise sa clef privée pour le déchiffrer

$$m = x^d \pmod{n}$$



Code RSA : exemple

Génération des clefs

On choisit $p = 5$ et $q = 17$

$n = p \times q = 5 \times 17 = 85$

$\varphi(n) = \varphi(85) = (p-1) \times (q-1) = 4 \times 16 = 64$

On prend $e = 5$ pour lequel on a bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(5, 64) = 1$

la clef publique est donc $(n = 85, e = 5)$

Théorème de Bezout

Si a et b sont des nombres premiers, il existe deux nombres entiers relatifs u et v tels que au+bv=1

Clef privée à partir de l'identité de Bezout

$5 \times 13 + 64 \times (-1) \equiv 1 \pmod{64}$

Donc $5 \times 13 \equiv 1 \pmod{64}$

$d = 13$ est la clef privée

Code RSA : exemple

Chiffrement

On veut chiffrer $m = 10$

$x = m^e \bmod n = 10^5 \bmod 85 \equiv 40 \bmod 85$

Donc $x = 40$

Déchiffrement

Pour déchiffrer $x = 40$

$m = x^d \bmod n = 40^{13} \bmod 85 \equiv 10 \bmod 85$

Edmonium

Cryptographie quantique

Il s'agit de la distribution quantique des clés

- ✓ On peut utiliser les propriétés quantiques de photons polarisés (protocole BB84, Bennet et Brassard 1984, E81)
- ✓ On peut utiliser l'intrication quantique de 2 photons
- ✓ On a une sécurité absolue

Propriétés quantiques utilisées :

- ✓ Réduction du paquet d'onde
- ✓ Phénomène d'intrication (quantum entanglement) : l'information se transmet plus vite que la lumière
- ✓ Théorème d'impossibilité du clonage quantique (impossible de copier à l'identique un état quantique inconnu et arbitraire)

Testé en 2002 sur une distance de 67 km (Genève-Lausanne). En 2017 le record est de 1400 km (Chine)

呆

Edmonium

7. Ingénierie sociale

吳

Edmonium

Ingénierie sociale

Exemple d'attaque classique

Hacker ⇒ Alice
Objectif ⇒ collecter des informations confidentielles pour un groupe étranger

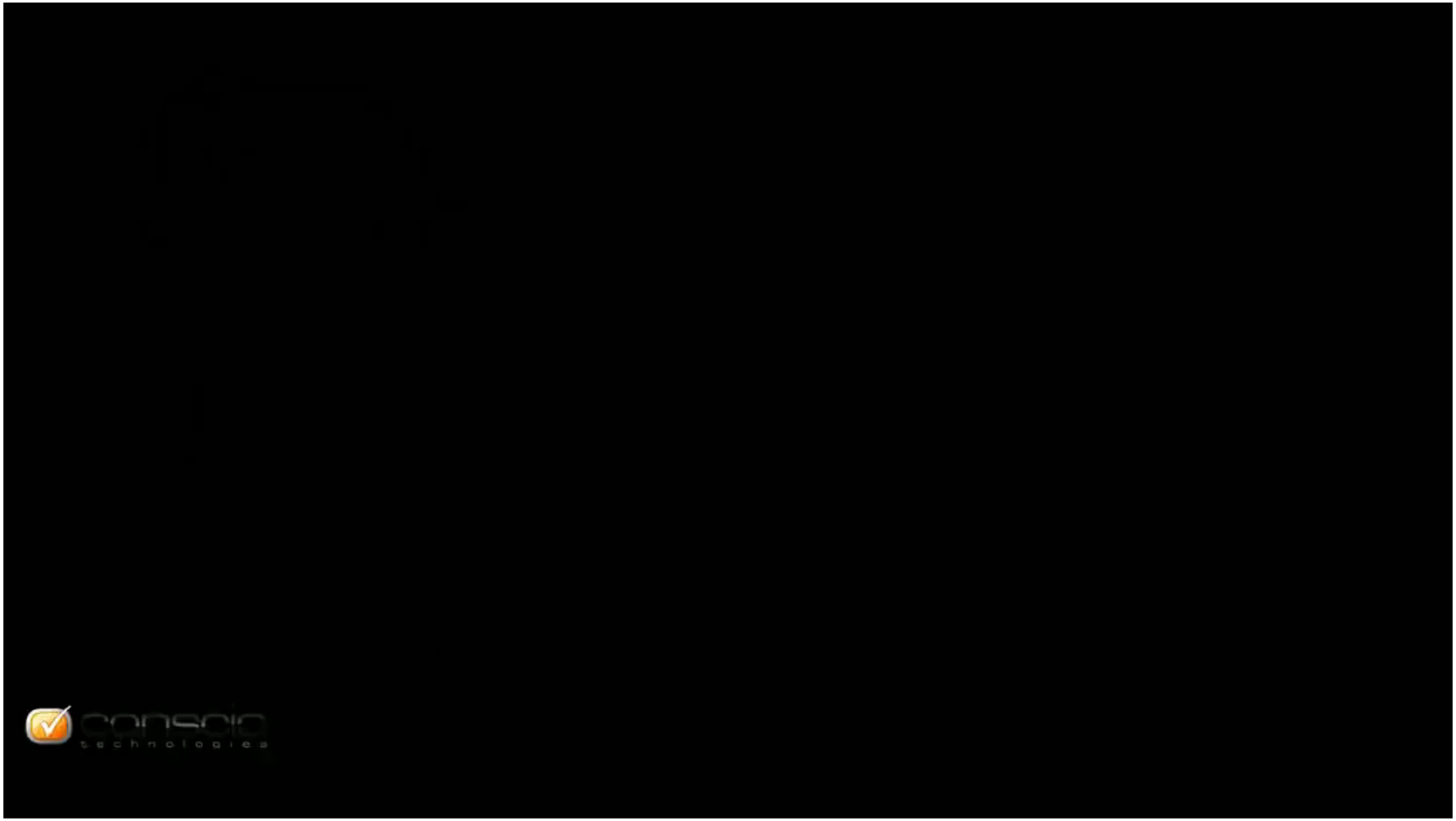
Étape 1 ⇒ Cible : Pierre (manager dans l'entreprise)

- Collecte d'informations sur lui et son entreprise (réseaux sociaux, forums, traces internet, etc.)
- Alice lui téléphone en se faisant passer pour une journaliste et en flattant son entreprise pour faire un article sur lui et son entreprise
- Avec toutes les informations recueillies, Alice va se faire passer pour Laura, collaboratrice dans une filiale de l'entreprise à l'étranger

Edmonium

Ingénierie sociale

Exemple d'attaque classique (http://www.conscio-technologies.com)
https://www.youtube.com/watch?v=IbetgF2f_58



吳

Edmonium

Ingénierie sociale

Précautions à prendre

https://www.youtube.com/watch?v=fuNqsFXqQOU&t=100s

Arnaque au président

https://www.youtube.com/watch?v=4kWvhFdiV3s

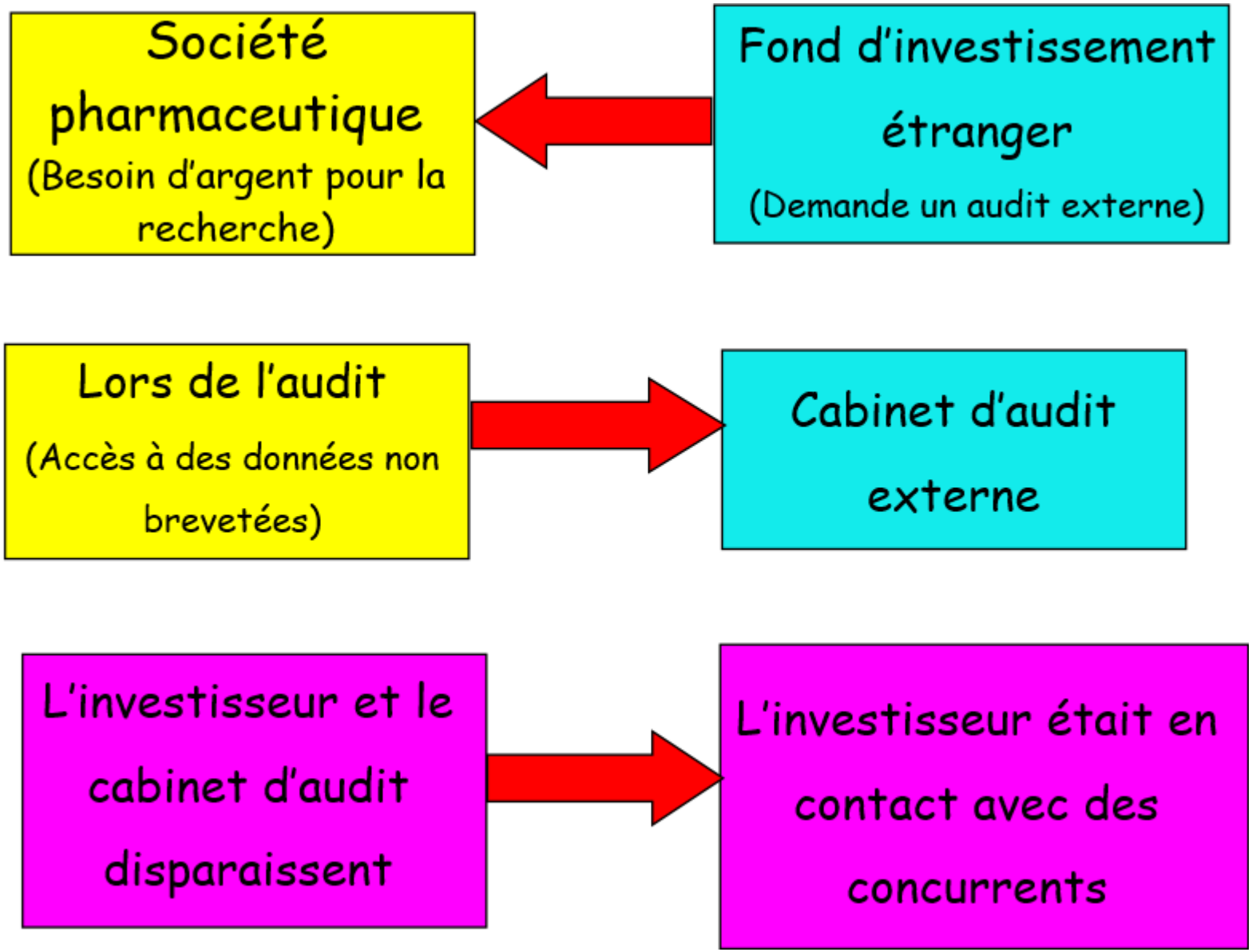
Edmonium

Arnaque sur le net

https://www.youtube.com/watch?v=ahMdDonLoC4&t=330s

吳

Les faux audits



Edmonium

Social engineering (mot de passe)

https://www.youtube.com/watch?v=_fGJrHFrw4E

吳

Arnaque par manipulation psychologique

https://www.youtube.com/watch?v=6cJyEEzqMzo

Edmonium

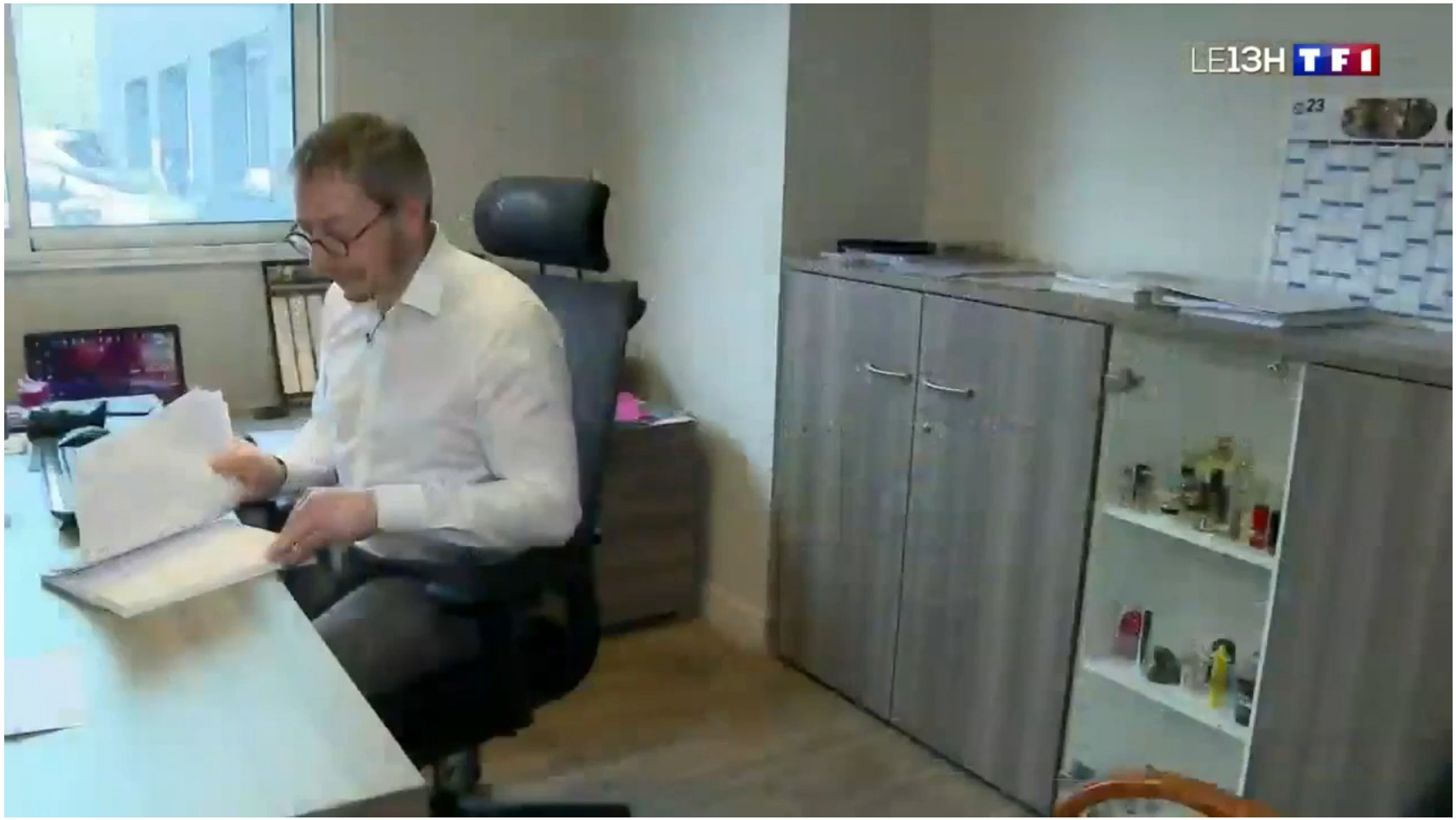
Décryptage d'un cas d'ingénierie sociale

https://www.youtube.com/watch?v=zc1jOBjwx3c

呆

Edmonium

Arnaque au président



https://www.youtube.com/watch?v=k04NvNQliGw

吳

Arnaque au président

https://www.youtube.com/watch?v=4kWvhFdiV3s

Edmonium

8. Bitcoin, blockchain

吳

Edmonium

Bitcoin et Blockchain

https://www.youtube.com/watch?v=du34gPopY5Y&t=328s

吳

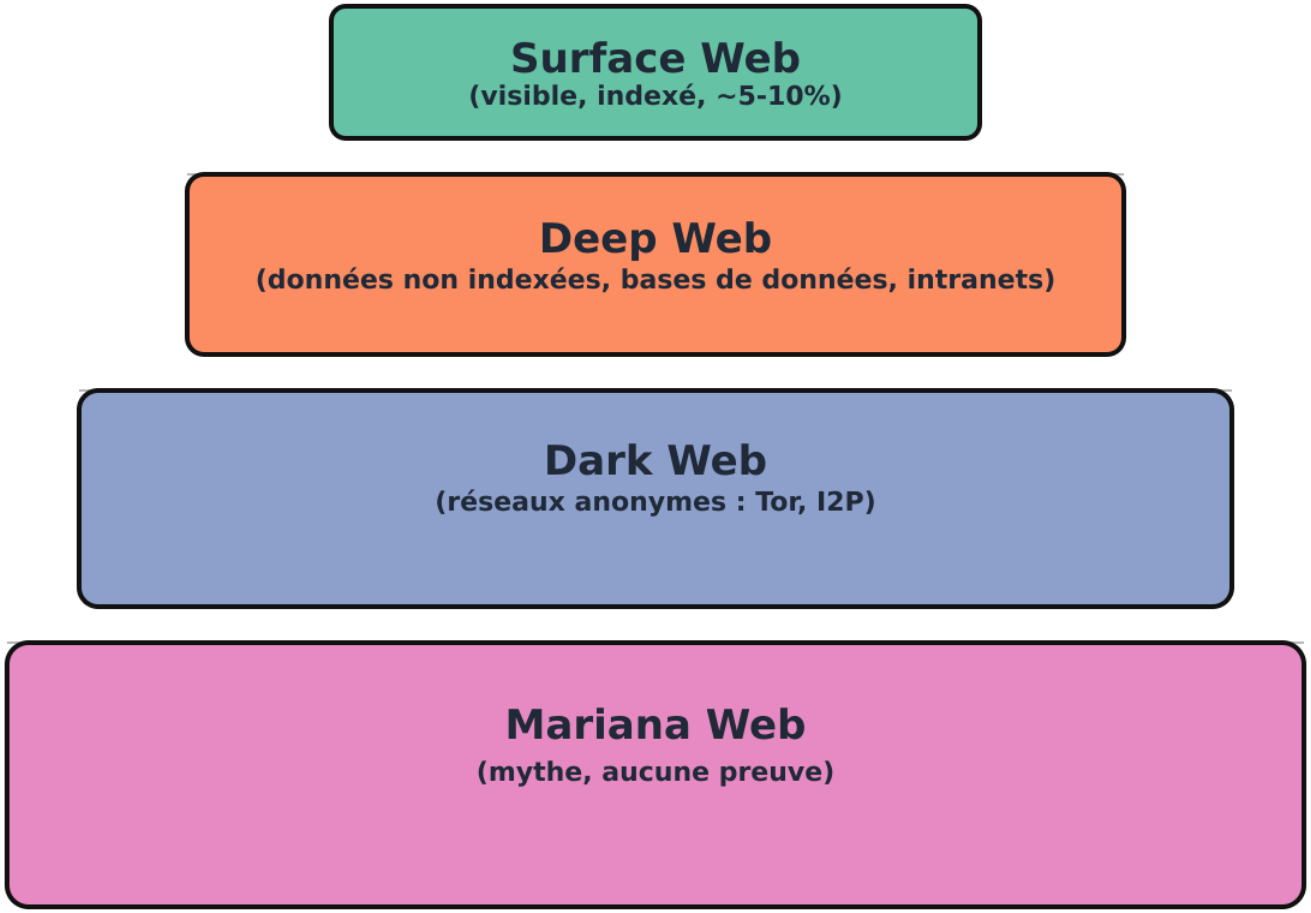
Edmonium

9. Deep web et dark web

吳

Edmonium

Pyramide des couches du Web



Le "Mariana Web" est une légende urbaine ; techniquement, tout contenu non indexé fait partie du Deep Web.

Edmonium

Deep Web, Darknet

https://www.youtube.com/watch?v=t0KVDG4etgo

呆

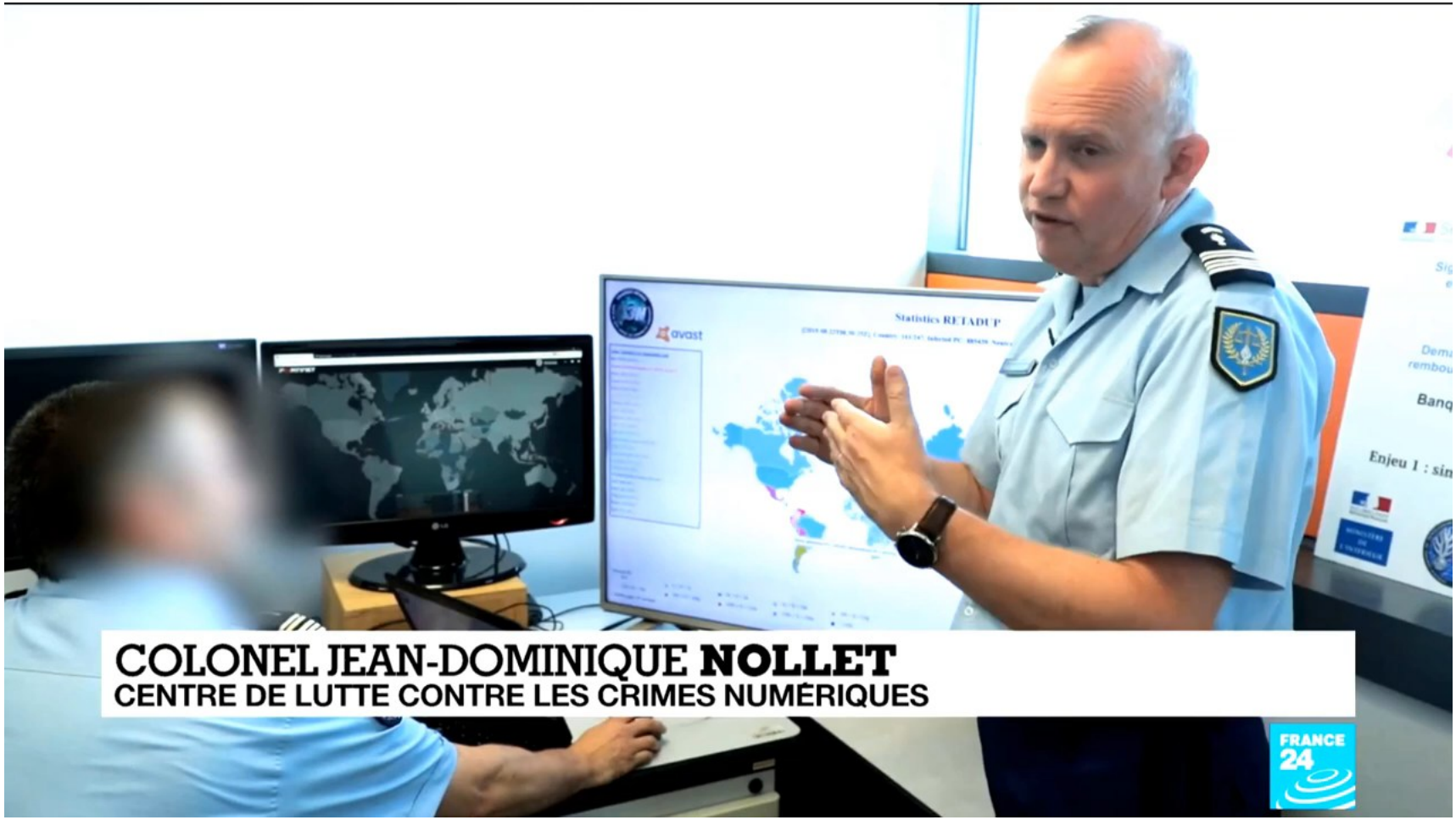
Edmonium

VPN
Virtual Private Network

https://www.youtube.com/watch?v=8rIS50kFwkA

吳

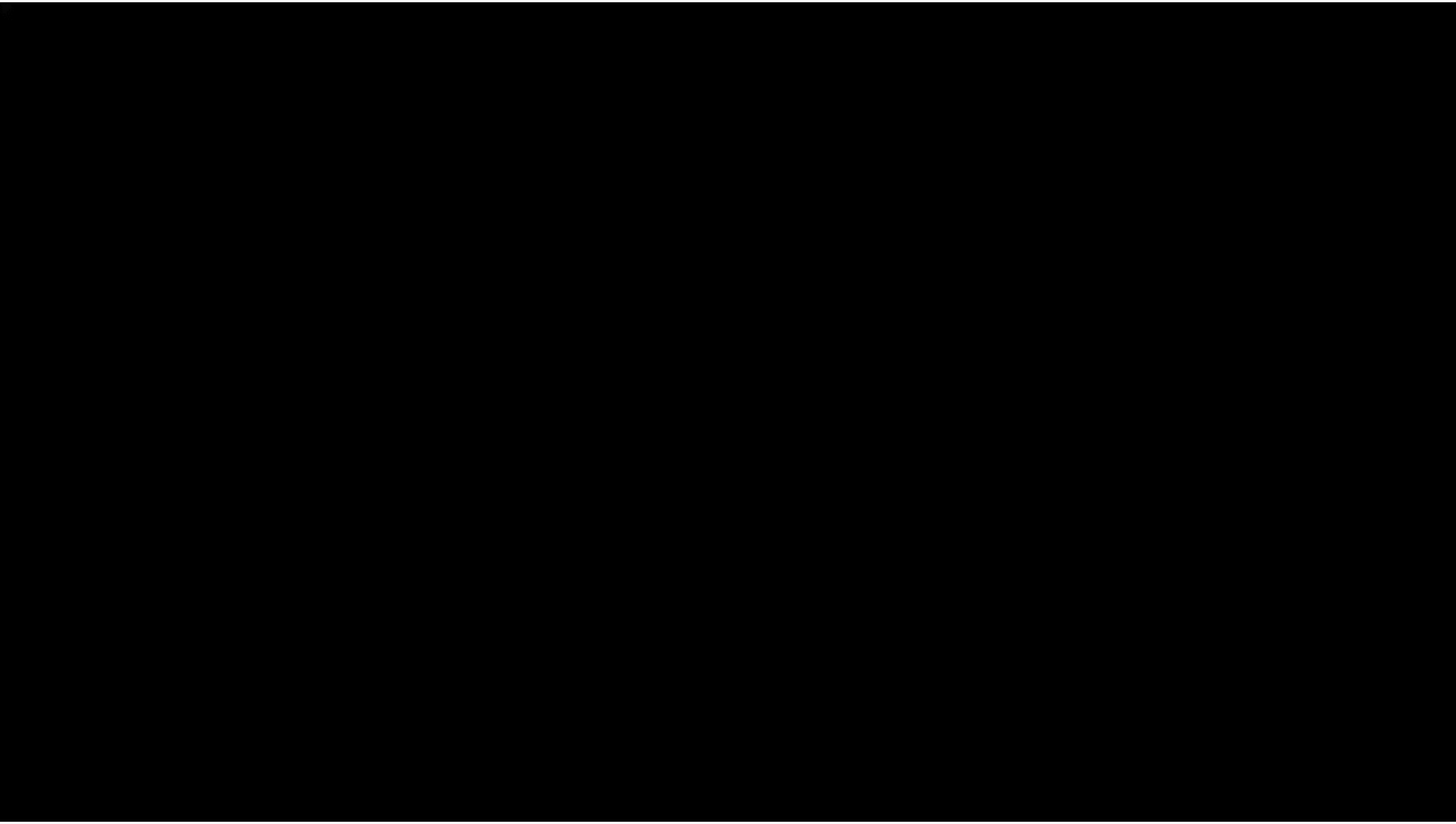
Les Botnets : armes de guerre numérique



https://www.youtube.com/watch?v=CMyVvqf_IIY

吳

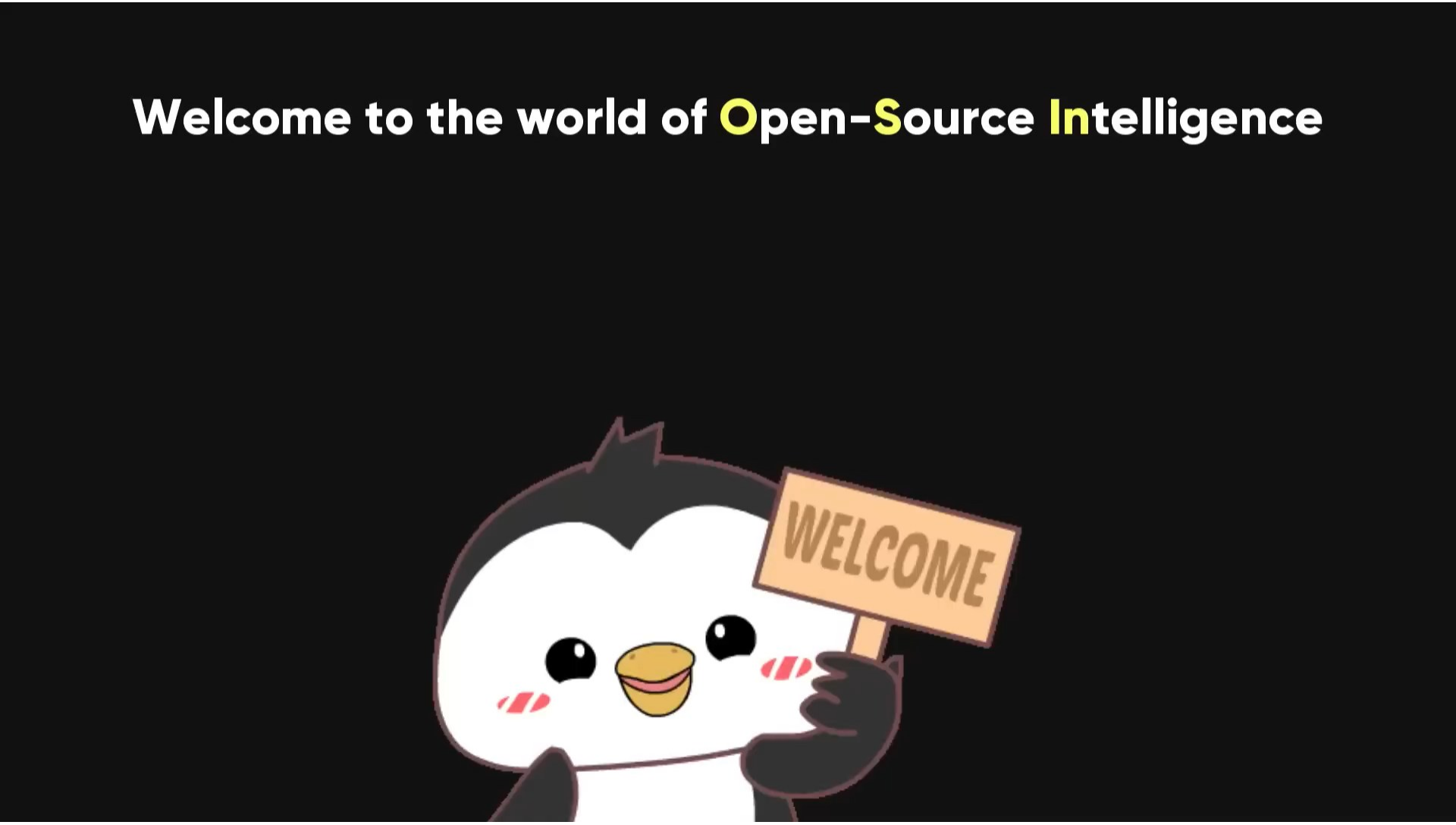
Cyberattaques



https://www.youtube.com/watch?v=MphsTB5PAEE

Edmonium

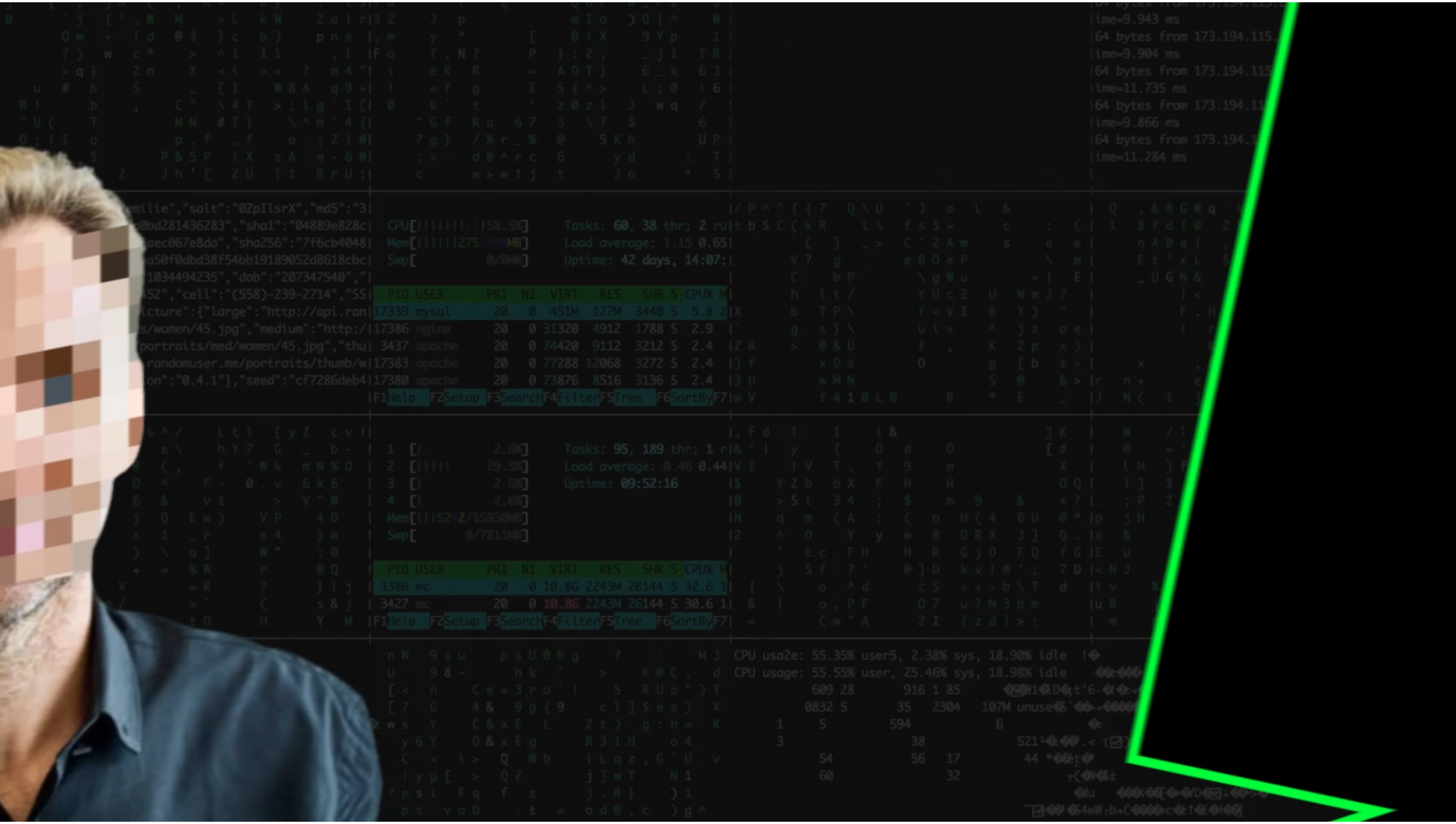
OSINT



https://www.youtube.com/watch?v=aD-U2kP0vNk

Edmonium

OSINT

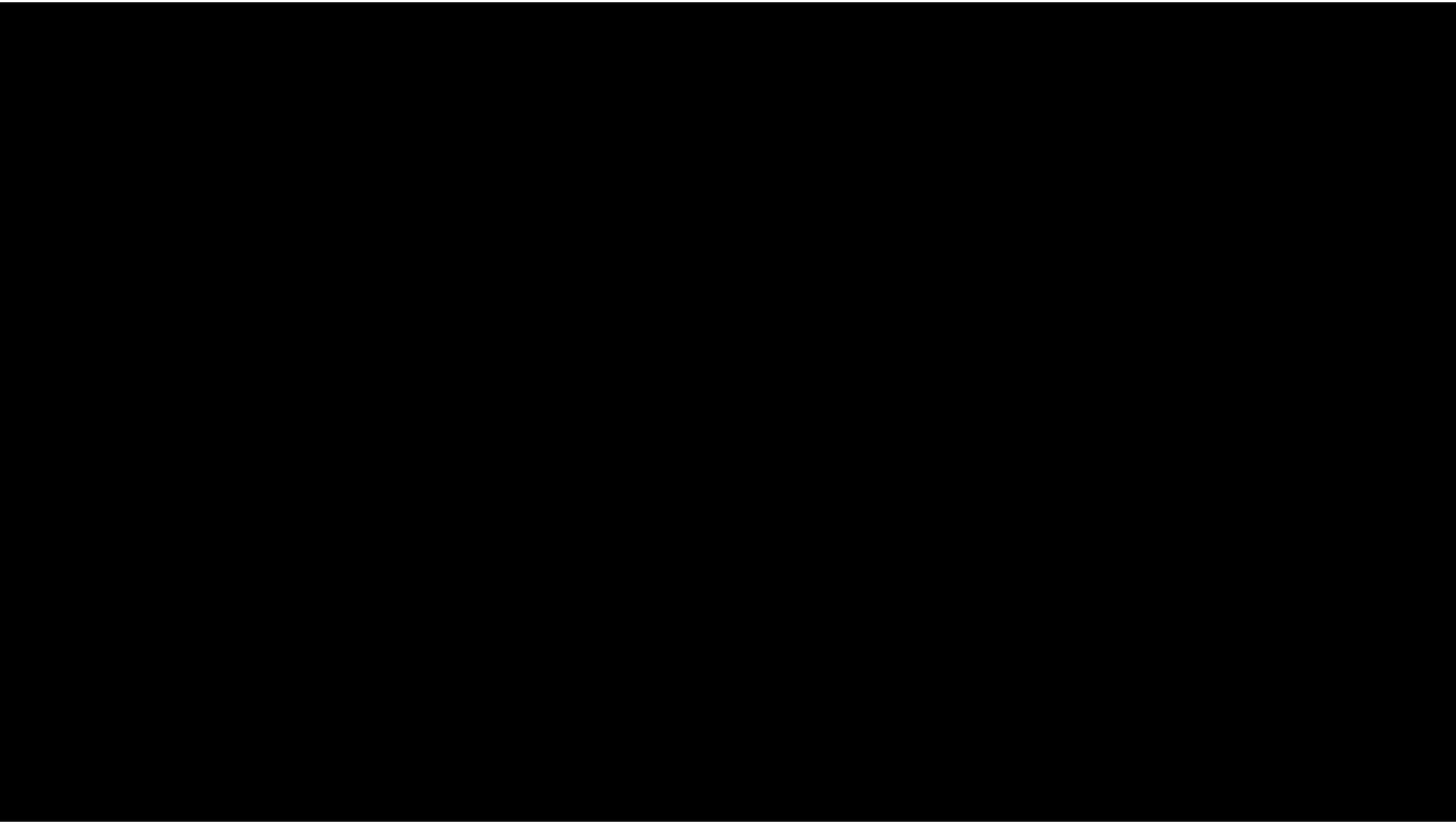


https://www.youtube.com/watch?v=rTCwJFkuxvI

吳

Edmonium

Erreur avec un VPN



https://www.youtube.com/watch?v=6f_0YLQbsWs

吳

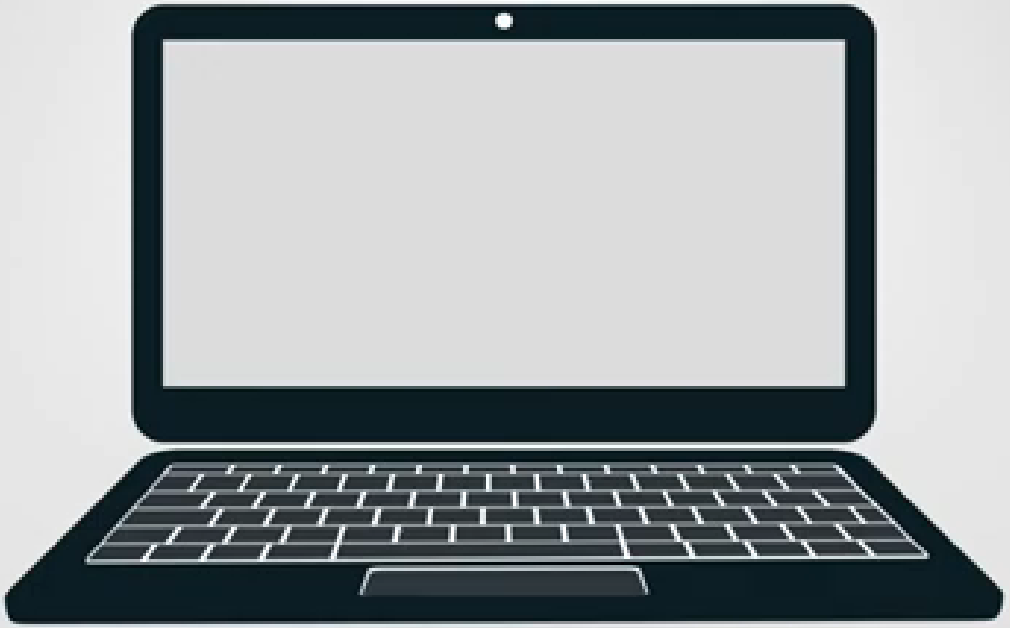
Edmonium

Arnaque nigériane

https://www.youtube.com/watch?v=nyYm56b2-y4

吳

Social engineering (mot de passe)



https://www.youtube.com/watch?v=S3kHbYdS9AE

吳