Séminaire OSINT 1

Recherche et exploitation d'informations sur internet

Artus Huot de Saint-Albin
Spin Partners

Artus Huot de Saint-Albin

- **Diplômes :**

- M1 Relations Internationales – Lyon III 2012 - 2013
- Master spécialisé IE – École de Guerre Économique 2013 - 2014

- **Expérience professionnelle :**

- Consultant, pôle études – Spin Partners 2014 - 2016
- Consultant, pôle influence – Spin Partners 2016 - 2018

#DueDiligence #Veille #OSINT #Cartographies

I. OSINT : concepts & finalités

1.1. Définition
1.2. Quelles finalités pour l'OSINT ?
1.3. Concentricité et rebond : deux logiques fondamentales
1.4. Le digital privacy paradox

II. Addons, bookmarklets & sites au service de l'OSINT

2.1. Addons
2.2. Bookmarklets
2.3. Sites spécialisés

III. Cas pratiques

I. OSINT : concepts & finalités

OSINT : Open Source Intelligence ou renseignements de sources ouvertes.

« **Informations non classifiées** qui ont été délibérément **découvertes**, **discriminées**, **distillées** et **diffusées** à un public choisi afin de répondre à une question spécifique ».

Robert David Steele, *Open Source Intelligence Analysis*

L'OSINT est, par définition, bornée au cadre légal. Ce même cadre légal établit la frontière entre intelligence économique et espionnage industriel.

Quelles finalités pour l'OSINT ?

- **La recherche**

- S'approprier un sujet en ayant les informations les plus pertinentes
- Réaliser une cartographie d'acteurs
- Trouver les coordonnées d'un expert

- **La protection de ses données**

- Évaluer et maîtriser l'information accessible sur soi/ son entreprise
- Accroître sa protection face aux menaces de type doxxing, usurpation d'identité, arnaque au président.

Doxxing : pratique consistant à rechercher et à révéler sur Internet des informations sur l'identité et la vie privée d'un individu dans le dessein de lui nuire.

Six catégories de sources

Médias
- Magazines, radio, télévision.

Internet
- Réseaux sociaux, blogs, forums, sites collaboratifs.

Données publiques gouvernementales
- Statistiques, budgets, registres, annuaires.

Publications scientifiques et professionnelles
- Comptes-rendus de conférences, thèses, travaux académiques.

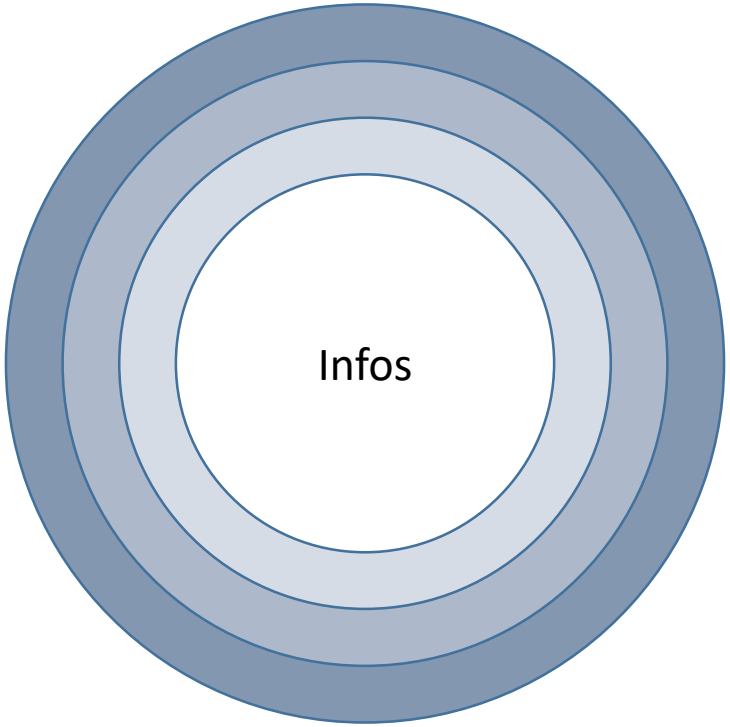
Données commerciales
- Bases de données, résultats financiers, bilans annuels, ratings.

Littérature grise
- Rapports techniques, brevets, newsletters.

Concentricité et rebond : deux logiques fondamentales

Sur le Web, chaque information peut mener à une nouvelle information, accentuant en même temps **les connaissances** et **les possibilités de recherches**.

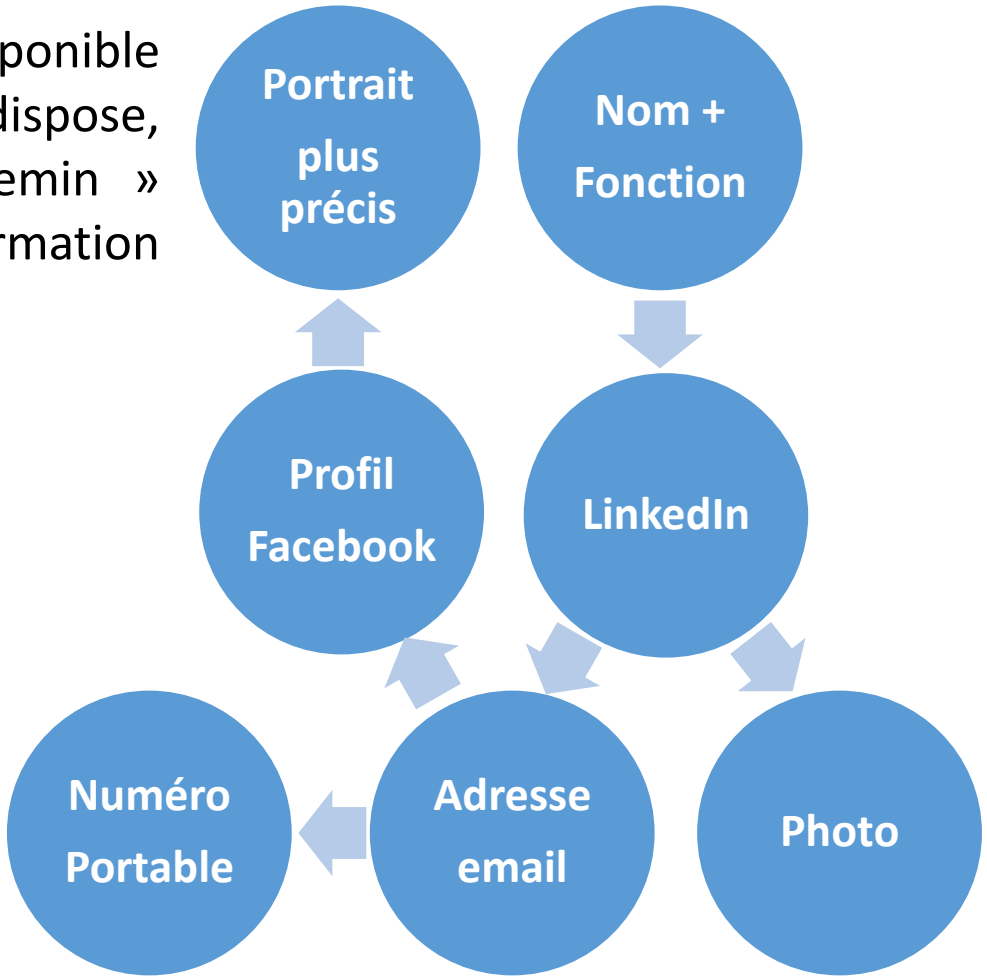
Périmètre du cercle = périmètre de recherche.



La logique de rebond

Si une information n'est pas disponible à partir des éléments dont on dispose, il convient d'établir un « chemin » permettant de mener à l'information recherchée.

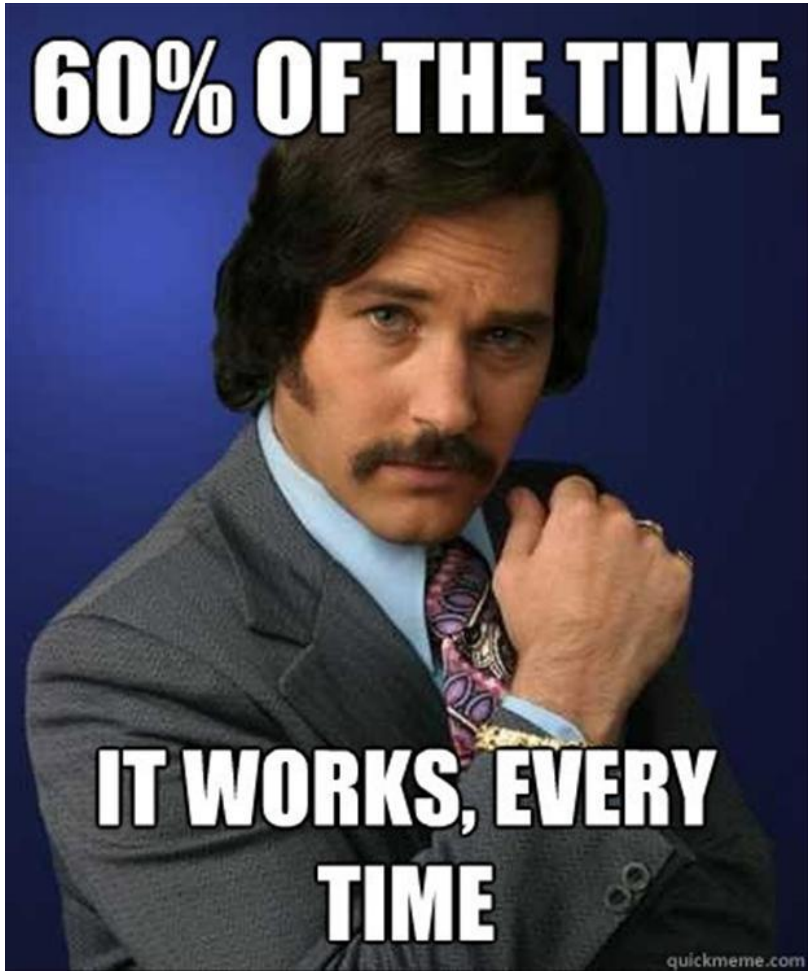
A → | D
A → B
B → C
C → D



Il n'existe pas d'outil miracle pour trouver une information

Chaque outil a un taux de réussite compris entre 1 et 99%.

Il est donc nécessaire de maîtriser une palette d'outils/ techniques la plus large possible.



Le « digital privacy paradox »

« *Quand vous interrogez les gens sur la protection de leur vie privée, ils expriment leur aversion face à la perte de celle-ci, mais ils ont tendance à ne pas faire les choix correspondant à ces préférences.* »

Susan Athey, professeur d'économie à Stanford

74% des Américains estiment que la sécurité de leurs données personnelles est « très importante »…

… et **98%** donnent leur adresse email en échange d'une part de pizza (étude réalisée auprès de 3 108 étudiants du MIT).

90% des Français se disent préoccupés par leurs données mises en ligne (CSA research).

II. Addons, bookmarklets & sites au service de l'OSINT

Avant d'entamer des recherches, il est nécessaire de configurer son navigateur afin :

- De gagner du temps
- D'accéder à des informations supplémentaires sur les pages visitées
- De renforcer sa sécurité et optimiser la navigation

Quelques extensions de recherche (Chrome ou Firefox)

- Hunter : trouver adresse mail correspondant à un domaine (100 requêtes/mois)
- Prophet : trouver RS/sites liés à un profil. Permet aussi de trouver d'anciens sites (requêtes illimitées)
- ContactOut : trouver l'adresse mail + numéro d'un profil LinkedIn (50 R/mois)
- Lusha : trouver l'adresse mail + numéro d'un profil LinkedIn (5 R/mois)

Les bookmarklets

Bookmarklets : programmes JavaScript insérés dans le navigateur (comme des raccourcis). Ils ont surtout vocation à faire **gagner du temps** en automatisant une tâche :

- FB ID : trouver l'identifiant Facebook depuis un profil
- FB Expand : dérouler une page Facebook automatiquement
- FB Comment : dérouler les commentaires des publications affichées
- Archive.org : consulter les archives d'un site
- Archiver : enregistrer une page sur Archive.org
- Wikipédia : ouvre la page Wikipédia d'un mot sélectionné
- Whois : ouvre le Whois d'un site sur domainetools.com

Les bookmarklets se trouvent sur le Web au moyen de requêtes Google ou peuvent être directement écrits par des personnes maîtrisant JavaScript.

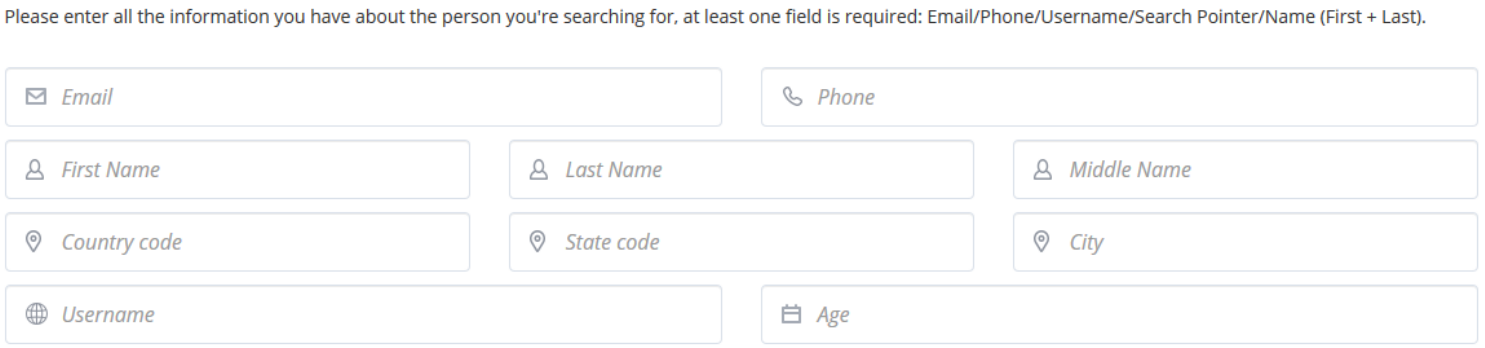
Les sites spécialisés

- IntelTechniques.com

IntelTechniques permet de **centraliser des équations de recherches** sur/ à partir :

- 25 moteurs de recherches
- Les plateformes collaboratives (Prezi, Slideshare, etc.)
- Les réseaux sociaux
- Des types de fichiers (PFD, Word, PPT, etc.)
- D'une adresse email
- D'un pseudonyme
- …

- Pipl.com/api/demo



Pipl est un moteur qui **explore le deep web** pour établir des connexions avec un élément préalablement renseigné (adresse email, numéro de téléphone, prénom, nom, pays, ville, pseudonyme, âge).

Pipl est un outil automatisé et peut générer des **faux-positifs**.

Il est donc nécessaire de **recroiser les informations**.

Effacer des informations de Pipl API Demo :

Écrire à : **mail@pipl.com**

Hi,

I used your service, Pipl API Demo (which is great btw), to check the information about me from my email address and I found that my phone number is displayed (link below). Is it possible to remove it or find out from which service/website you got it ?

https://api.pipl.com/search/v5/?email=********@gmail.com&key=sampleyeakhicep2mrcm66fd&pretty=true

Thank you,

III. Cas pratiques

Objectif : à partir d'informations de base (nom + prénom), vérifier si son numéro de téléphone et son email sont publics.

Outils utilisés :

- LinkedIn
- Contact Out
- Pipl API Demo
- WhatsApp

Cas pratique

Objectif : vérifier si son compte Facebook (même anonymisé au moyen d'un pseudonyme) est facilement accessible, puis consulter les informations pouvant être collectées par un tiers ne faisant pas partie de ses amis.

Outils utilisés :

- Pipl
- IntelTechniques

Récapitulatif des outils et sites

Sites :

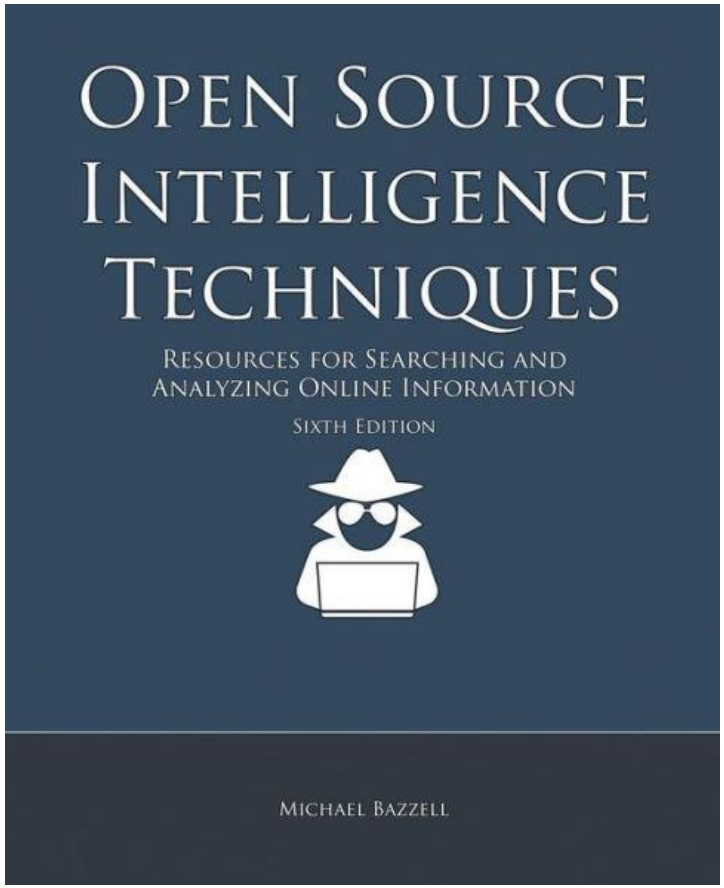
- www.inteltechniques.com
- www.pipl.com/api/demo
- www.recruitin.net
- www.mailtester.com
- www.peoplefindthor.dk

Extensions :

- Hunter
- Prophet
- ContactOut
- Lusha

MERCI DE VOTRE ATTENTION !

Pour aller plus loin



@Usurp_ID
@Securite_eco
@artushsa

@Capteur_Ouvert
@secou
@technisette
@bellingcat

@jakecreps
@navlys_
@Sector035
@jnordine

#OSINT

https://medium.com/week-in-osint
https://start.me/p/wMdQMQ/tools
https://osintframework.com

https://inteltechniques.com (Forum)

AEGE - Le réseau d'experts en intelligence économique

aege.fr

contact@aege.fr

portail-ie.fr

contact@portail-ie.fr

196, rue de Grenelle, 75007 Paris
+33 1 45 51 00 02