# Rapport : Pour une meilleure gouvernance de l'OSINT

Category: 2020-2030,Actualités,Renseignement
9 décembre 2024

**Rapport Synopia**
**(novembre 2024)**

**En novembre 2024, Synopia, grâce au travail de son groupe d'experts de haut niveau, a publié son 2e rapport sur l'OSINT (*Open Source Intelligence*). Nous en présentons ici un résumé**.

**Commentaire AASSDN** : Le *Think tank Synopia* qui prend une place croissante dans la réflexion sociétale et stratégique vient de publier son deuxième rapport sur l'*Osint*. En quelques années le renseignement par sources ouvertes a quitté les rives des spécialistes du cyber et devenir essentiel pour les Administrations, les Services et les Entreprises. Au-delà de la technique et des outils il est réconfortant de voir que l'analyste, l'homme croisant expérience et intuition, est le maillon clé à condition qu'il ne se laisse pas submerger par l'émotion, les *a priori* et les idéologies.

Le problème est que, contrairement à beaucoup d'acteurs étrangers de tous ordres, tous n'ont pas mesuré l'utilité de ce moyen révolutionnaire qui permet de comprendre et d'anticiper. Il suffit de lire ou d'écouter les médias pour comprendre que la majorité des journalistes l'ignorent, que nos Services ont toujours du mal à intégrer une approche qui remet en cause leurs méthodes traditionnelles, et que la plupart de nos responsables politiques ne savent pas comment utiliser cet apport essentiel pour comprendre le monde réel.

La guerre est devenue hybride, et nous n'avons pas d'amis. Dans le monde de l'information il faut savoir se battre contre les actions de toutes origines qu'elles soient d'influence de désinformation ou subversives.

L'OSINT, dont l'importance a été mise en lumière avec le conflit russo-ukrainien, consiste à utiliser une multitude d'informations accessibles en ligne pour en extraire des renseignements sur des individus, des groupes, des produits, des entreprises et des organisations militaires.

Ce processus nécessite de disposer d'**analystes qualifiés**, maîtrisant les techniques d'exploration de données et dotés d'un esprit critique pour évaluer avec précision la fiabilité et la pertinence de ces données. Mais **l'OSINT nécessite surtout de disposer de capteurs et des logiciels** qui aident les analystes à collecter, traiter et analyser plus efficacement les données de source ouverte.

Sur le plan étatique, une **vraie prise en compte de l'OSINT s'est opérée ces dernières années au sein des services de renseignement et des administrations**. Cependant, c'est au sein des entreprises privées qu'ont eu lieu les évolutions les plus importantes. En effet, au niveau commercial et entrepreneurial, **l'OSINT est devenue un instrument essentiel de l'aide à la décision**, en particulier dans le domaine de la veille concurrentielle.

En revanche, au niveau des services de l'État, l'OSINT demeure encore **un complément d'information délicat à intégrer dans la manouvre du renseignement** et parfois regardé avec méfiance, souvent par manque de formation, ou par « culture ».

La plupart du temps **utilisé de façon défensive dans notre pays**, l'information en source ouverte constitue cependant un puissant levier de la **guerre informationnelle** au travers de ses capacités d'influence, de **manipulation des esprits** (cognitif) et de **fabrication de narratifs** ou de contre-narratifs.

De nombreux pays alliés ont bien compris la **menace asymétrique** qu'il constituait et ont développé des programmes de coopération internationale, notamment pour lutter contre le terrorisme. **Mais il reste beaucoup à faire pour tirer le meilleur profit de l'OSINT**, en France comme en Europe. Le travail mené pendant deux ans par Synopia a permis de mettre en lumière la multiplicité des usages de l'OSINT, la diversité des sources d'information et la rapidité stupéfiante des évolutions technologiques.

L'application du principe de l'OSINT aux données web peut être représentée par une chaîne de valeur en six composantes, chacune assumée par des acteurs différents :

- Moteur de recherche web
- Veille web
- Alerte temps réel sur le web
- Protection du risque humain sur le web
- Influence ou contre-influence web
- Stratégie fondée sur des données web

Chaque composante peut ensuite être comprise selon trois grandes étapes de traitement des données : **le questionnement, la collecte et l'analyse**.

Des attributs transverses peuvent être associés aux solutions d'OSINT :

- Renseignement défensif et/ou offensif
- Renseignement d'origine ou d'intérêt cyber
- Enjeu de discrétion
- Enjeu de souveraineté numérique

En parallèle des enjeux techniques et opérationnels, deux autres domaines sont apparus comme essentiels :

- La formation

Il existe de multiples formations OSINT, qui consistent en l'apprentissage de techniques pour **collecter et analyser les informations publiques, et effectuer une veille stratégique**. Certaines formations apprennent également à **se prémunir des conséquences d'une analyse trop parcellaire**, partisane ou incorrectement sourcée pour une entreprise ou une institution. L'OSINT est enseigné aussi bien de manière offensive que défensive.

Notre rapport dresse un inventaire des principales formations en OSINT.

- Le cadre juridique

Les aspects juridiques, en perpétuelle évolution, sont à appréhender avec rigueur si l'on veut **rester dans le cadre légal mais aussi éthique**. Les outils de l'OSINT et l'information à laquelle ils donnent accès doivent respecter les contraintes légales et réglementaires applicables, notamment concernant la protection de la vie privée, la gestion des données, l'utilisation d'avatars et l'extra-territorialité. Là encore, **la formation des utilisateurs et des destinataires de l'OSINT est nécessaire, de même que le recours aux spécialistes** de ces enjeux très pointus (avocats, juristes et professeurs de droit). Le rapport Synopia traite ainsi des différents moyens envisageables qui permettraient d'optimiser l'utilisation de l'OSINT et **Synopia recommande qu'une impulsion politique forte structure la filière de l'OSINT**, afin de permette à l'État de mieux s'adapter aux évolutions technologiques, voire de les anticiper, et de mieux intégrer les innovations technologiques dans les processus décisionnels, en prenant garde à bien en garder le contrôle. Il en va de sa souveraineté. **Le rapport souligne aussi l'importance de préserver la liberté d'action des différentes entités** pour leur permettre de s'adapter à ce domaine si évolutif.

Pour en savoir plus, contactez Synopia : **synopia@synopia.fr**

Synopia
20, rue Georges Bizet
F-75116 Paris
www.synopia.fr