ChatGPT

Dossier pédagogique : introduction à l'OSINT (Open Source Intelligence)

Introduction : qu'est-ce que l'OSINT ?

Le terme **OSINT (Open Source Intelligence)** désigne le processus d'**exploitation de sources d'information ouvertes pour produire du renseignement**. Selon des sources institutionnelles, l'OSINT repose sur la **collecte, l'évaluation et l'analyse de données librement accessibles pour répondre à des besoins précis** [1]. Il ne suffit pas de consulter des informations publiques : l'OSINT implique de transformer ces données éparses en **produits de renseignement exploitables**. La loi américaine, souvent citée en référence, précise qu'un renseignement ouvert est constitué d'« informations disponibles au public, collectées, analysées et diffusées en temps opportun pour répondre à un besoin spécifique » [2].

Les sources utilisées couvrent un large spectre : registres publics, médias d'actualité, bibliothèques en ligne, réseaux sociaux, images et vidéos partagées sur Internet, fichiers historiques archivés, mais aussi les sections moins visibles du Web (deep web) et certaines zones accessibles du dark web [1]. Parce qu'elle s'appuie sur des sources ouvertes, la discipline est souvent perçue comme un outil démocratisant le renseignement, accessible à des journalistes, des ONG ou des analystes indépendants. Toutefois, l'interprétation et la validation des informations demeurent essentielles pour produire un renseignement fiable, comme le rappelle la nécessité de vérifier les rumeurs en contexte de crise [3].

Brève histoire de l'OSINT

- **XIX^{e} siècle : premières pratiques** : dès la guerre de Sécession américaine, les deux camps utilisaient les journaux et les documents publics pour suivre les mouvements adverses [4]. L'OSINT existait donc avant l'arrivée des nouvelles technologies, sous forme de surveillance des médias imprimés et de collecte d'informations publiques.

- **Seconde Guerre mondiale et Guerre froide** : le Royaume-Uni créa le **BBC Monitoring** en 1939 pour écouter et analyser les émissions radio étrangères, ce qui permit de surveiller la propagande et les communications adverses [5]. Aux États-Unis, le **Foreign Broadcast Monitoring Service (FBMS)** fondé en 1941 fut chargé de surveiller les émissions de radio des puissances ennemies ; il devint par la suite la **Foreign Broadcast Information Service (FBIS)** qui étendit sa collecte à tous les médias mondiaux [6].

- **1980-1990 : reconnaissance institutionnelle** : le terme « OSINT » fut adopté par les services de renseignement américains à la fin des années 1980, alors que le développement d'Internet et la démocratisation de l'informatique multipliaient les sources ouvertes [7]. Les agences et les armées ont commencé à structurer l'acquisition d'outils et de méthodologies dédiés, avant que ces pratiques ne se diffusent plus largement dans les médias et la société civile.

- **Années 2000 et 2010 : explosion des données** : l'avènement des réseaux sociaux, des bases de données ouvertes et du big data a transformé la discipline. Les journalistes d'investigation ont

adopté les techniques OSINT pour accéder à des informations jadis réservées aux services de renseignement [8]. Des organisations de défense des droits humains ont également développé des protocoles (comme le **Berkeley Protocol**, publié en 2020) afin de garantir la fiabilité et la valeur juridique des preuves collectées sur Internet [9].

Domaines d'application de l'OSINT

Sécurité informatique et cybersécurité

Dans le domaine de la cybersécurité, l'OSINT sert à **détecter des menaces et identifier des vulnérabilités**. Les analystes collectent des informations issues de sites web, d'articles, de forums, de réseaux sociaux et de bases de données pour évaluer le risque, par exemple en recherchant des fuites de données, des adresses IP exposées ou des comptes compromis [10]. Le cycle de renseignement appliqué à la cybersécurité inclut :

1. **Planification et orientation :** déterminer les menaces à surveiller et définir les besoins d'information [11].
2. **Collecte :** utiliser des moteurs de recherche avancés, des services d'indexation des objets connectés (par exemple **Shodan**) ou des outils de corrélation (par exemple **Maltego**) pour rassembler des données [12].
3. **Traitement :** filtrer et structurer les données pour les rendre exploitables.
4. **Analyse :** identifier des schémas, des indicateurs d'attaque ou des relations entre les acteurs ; évaluer les capacités des attaquants et leur modus operandi [11].
5. **Diffusion :** transmettre les rapports aux décideurs et équipes de réponse afin de renforcer la défense informatique.

L'OSINT permet aussi aux pentesters et aux red teams de **collecter des informations sur les cibles** pour effectuer des tests d'intrusion ou des exercices d'ingénierie sociale. Toutefois, l'utilisation d'outils OSINT doit respecter les cadres juridiques, notamment en matière de protection de la vie privée [13].

Journalisme et vérification de l'information

Le journalisme d'investigation a adopté l'OSINT pour **vérifier des images, suivre des flux financiers ou cartographier des évènements**. Grâce à l'accès à des bases de données d'entreprises, des archives gouvernementales et des réseaux sociaux, les journalistes peuvent reconstituer des réseaux d'influence, traquer des navires ou analyser des vidéos de conflits [8]. L'ère numérique a multiplié les données (plusieurs centaines de milliards de gigaoctets de données générées par an), nécessitant des techniques OSINT pour trier et analyser ces volumes [8].

Des guides comme le **Verification Handbook** rappellent qu'en période de crise, de nombreuses rumeurs se propagent et que **la vérification des images et témoignages en ligne est cruciale pour délivrer une information fiable** [3]. Les journalistes utilisent notamment :

- La recherche inversée d'images et l'analyse des métadonnées pour authentifier des photos ou vidéos.
- La consultation de registres publics (immatriculations, archives de sociétés) pour vérifier des déclarations.
- La géolocalisation via des cartes et des imageries satellites.

Enquêtes privées et lutte contre la criminalité

Les enquêteurs privés et les juristes utilisent l'OSINT pour **reconstituer des profils, retracer des relations ou documenter des fraudes**. Les sources incluent les réseaux sociaux, les bases de données légales, les journaux locaux et les archives en ligne. Par exemple, les enquêteurs travaillant sur la **traite des êtres humains et le trafic de migrants** analysent les annonces publiées sur des forums, les réseaux sociaux ou les plateformes de petites annonces pour identifier les recruteurs et cartographier leurs connexions [14]. Ils peuvent croiser ces informations avec des données d'entreprises pour suivre les flux financiers et identifier les entreprises de façade [15]. L'ONUDC (Office des Nations Unies contre la drogue et le crime) souligne que ces investigations doivent respecter la confidentialité des victimes, que les informations doivent être vérifiées et que les enquêteurs doivent assurer leur propre sécurité en ligne [16].

Droits humains et justice internationale

Les ONG et organisations de défense des droits humains s'appuient sur l'OSINT pour **documenter des violations et collecter des preuves**. Le **Berkeley Protocol** définit des normes professionnelles pour l'identification, la collecte, la préservation et la vérification d'informations numériques, afin qu'elles soient recevables par les tribunaux [17]. Ce protocole est utilisé par des procureurs ukrainiens pour documenter des crimes de guerre et s'accompagne d'un guide destiné aux juges et avocats (2024) [9]. L'OSINT permet de :

- Analyser des vidéos et images provenant de témoins.
- Géolocaliser des sites de violations (bombardements, massacres).
- Croiser des données de réseaux sociaux pour identifier les auteurs d'atrocités.

Renseignement militaire et sécurité nationale

Les armées et services de renseignement ont longtemps utilisé l'OSINT pour compléter leurs sources classifiées. Dans le **National Defense Authorization Act 2025** américain, une disposition encourage l'US Army à **standardiser l'acquisition d'outils OSINT** pour analyser des articles de presse et des publications sociales afin de comprendre l'environnement sécuritaire [18]. L'article précise que des flux massifs d'informations publiques (réseaux sociaux, blogs, journaux) peuvent fournir des indications sur les mouvements de troupes et le moral des adversaires [19]. L'OSINT est donc devenu un composant essentiel du renseignement militaire moderne.

Ressources pour s'initier à l'OSINT

Cours et formations gratuites (MOOC)

Ressource	Description et points clés
Basel Institute on Governance – Cours OSINT	Cours en ligne gratuit et auto-rythmé menant l'apprenant à enquêter sur la pêche illégale. Il couvre la recherche sur Internet, les bases de données ouvertes, les réseaux sociaux, la navigation sur le deep web et la blockchain. Le cours met l'accent sur la préparation (organisation d'un plan de collecte), l'anonymat et la production d'un rapport final [20] [21].

Ressource	Description et points clés
Security Blue Team – Introduction to OSINT	Formation gratuite d'environ cinq heures comprenant neuf leçons. Elle enseigne le cycle du renseignement, la sécurisation de ses recherches en ligne, des outils et services courants et propose un projet final. Accessible en plusieurs langues, elle s'adresse aux débutants en renseignement de sécurité ou en enquêtes [22] [23] .
Basel LEARN – Open-Source Intelligence Course	Programme auto-rythmé de neuf sessions (~5 heures) disponible en plusieurs langues. Il enseigne les fondamentaux, la création d'un environnement sécurisé, la recherche sur l'open et le deep web, l'analyse des enregistrements de domaine, l'extraction de métadonnées, l'étude des communautés en ligne et la rédaction de rapports. Conçu pour des enquêteurs financiers, des journalistes ou des chercheurs sans expérience préalable [24] [25] .
Kapsuun Group – OSINT Beginners Course	Formation préparatoire gratuite en 18 leçons (environ une heure de vidéo). Elle aborde les bases de l'Internet (différence entre navigateur et moteur de recherche), les outils de capture (screenshot, vidéo) et l'utilisation des réseaux sociaux. Elle vise les novices souhaitant comprendre l'environnement du Web avant d'aborder des cours avancés [26] [27] .
Class Central (listes de cours)	Répertoire de plus de cent cours et certifications OSINT proposés sur des plateformes diverses (Udemy, YouTube, Cybrary). Les cours offrent des formations pratiques en investigation numérique (analyse des réseaux sociaux, géolocalisation, techniques de recherche avancée) pour des niveaux variés, avec des contenus gratuits et payants [28] .

Ouvrages recommandés pour débuter

Plusieurs livres constituent des bases solides pour les débutants. Voici une sélection avec des indications sur le public visé :

- **Michael Bazzell –** ***Open Source Intelligence Techniques*** : un manuel reconnu (10e édition) qui décrit des méthodes avancées de collecte et d'anonymisation. Il est destiné aux utilisateurs intermédiaires à avancés et propose des tutoriels détaillés sur la recherche d'informations en ligne [29] . Les débutants peuvent l'utiliser en référence, notamment pour apprendre des procédures pas à pas.

- **Rae Baker –** ***Deep Dive : Exploring the Real-world Value of Open Source Intelligence*** : cet ouvrage accessible explique les méthodes OSINT actuelles avec des études de cas réalistes. Il est recommandé pour les novices et les praticiens intermédiaires car il présente les concepts de manière claire et contextualisée [30] .

- **Joshua Picolet –** ***Operator Handbook : Red Team + OSINT + Blue Team Reference*** : guide polyvalent combinant des concepts d'équipes rouges, de renseignement ouvert et de défense (blue team). Utile pour les professionnels de la cybersécurité souhaitant relier OSINT et pratiques défensives [31] .

- **Brett Shavers – *Hiding Behind the Keyboard*** : ce livre s'adresse aux enquêteurs devant assurer leur anonymat et expliquer comment repérer des identités masquées. Il est utile pour des contextes d'enquête et de cybersécurité [32] .

- **Paul Troncone & Carl Albing – *Cybersecurity Ops with Bash*** : un ouvrage technique qui apprend à automatiser des tâches OSINT au moyen de scripts Bash. Il s'adresse à ceux qui possèdent déjà des bases en ligne de commande et souhaitent automatiser leurs recherches [33] .

Le blog **OSINTTeam** propose également une liste de livres classés par domaine (enquêtes numériques, journalisme, sécurité, etc.). Il conseille aux débutants de commencer par les ouvrages de Michael Bazzell ou par *Deep Dive* de Rae Baker pour une vision claire des méthodes et des outils [34] [35] . Le blog souligne l'importance d'aligner le choix du livre avec ses objectifs (journalisme, cybersécurité, droit) [36] .

Sites web, blogs et communautés

- **Bellingcat.com** : plateforme d'enquêtes open source célèbre pour ses travaux sur les conflits et la désinformation. Le site publie des guides méthodologiques et des études de cas qui illustrent comment utiliser des cartes, des vidéos et des données publiques pour enquêter.

- **IntelTechniques.com (Michael Bazzell)** : fournit des outils et des ressources actualisées pour la collecte d'informations, ainsi que des podcasts et des cours (souvent en anglais). Mentionné comme une référence pour apprendre les techniques OSINT [37] .

- **OSINT Framework (osintframework.com)** : annuaire interactif de ressources OSINT gratuites. Les outils sont classés par catégories (personnes, réseaux sociaux, images, domaines, etc.) et des icônes indiquent s'ils nécessitent un enregistrement ou un travail manuel [38] .

- **Forums et communautés** : de nombreuses communautés en ligne (Reddit r/OSINT, Discords spécialisés) permettent d'échanger des astuces, de partager des outils et d'obtenir des retours sur des enquêtes. Les articles de Social Links conseillent de rejoindre ces communautés pour pratiquer et mettre à l'épreuve ses compétences [39] .

Conseils pratiques pour débuter

1. **Établir une méthodologie** : commencez par définir votre question de recherche et vos objectifs (cycle de renseignement), puis élaborez un plan de collecte en identifiant les sources pertinentes. Utilisez un tableau ou un outil de gestion pour organiser les informations.

2. **Sécuriser ses recherches** : l'OSINT implique de naviguer sur des sites potentiellement malveillants. Utilisez un ordinateur dédié, des machines virtuelles, un VPN et des navigateurs anonymisés. Des guides comme ceux du Basel Institute insistent sur l'importance de protéger son identité numérique [40] [25] .

3. **Vérifier et croiser les sources** : comparez les données provenant de plusieurs sources avant de tirer des conclusions. Les manuels de vérification soulignent que les rumeurs et les fausses informations prolifèrent en période de crise [3] .

4. **Respecter la loi et l'éthique** : l'usage d'OSINT doit respecter les législations sur la vie privée et la protection des données. Par exemple, l'article de GDIT rappelle la nécessité de se conformer au

droit et de connaître les limites juridiques, notamment la protection des communications privées [13].

5. **Pratiquer régulièrement** : comme le recommandent les blogs et cours, créez un **laboratoire OSINT** personnel pour tester des outils, suivez des exercices pratiques (CTF, challenges) et participez à des communautés pour rester informé des nouveautés [39].

Conclusion

L'OSINT est une discipline en plein essor qui consiste à **transformer des informations ouvertes en renseignement fiable et exploitable**. Ses origines remontent aux premiers usages des journaux et de la radio pour collecter des données, et elle s'est développée avec l'avènement d'Internet et des réseaux sociaux. Aujourd'hui, l'OSINT est indispensable dans des domaines variés : **cybersécurité, journalisme, enquêtes privées, défense des droits humains et renseignement militaire**. De nombreux cours gratuits, livres et communautés permettent de s'y initier. Toutefois, la réussite d'une enquête OSINT repose sur une méthodologie rigoureuse, la vérification des sources et le respect des règles éthiques. En acquérant ces compétences, même un débutant peut exploiter la richesse des données ouvertes pour produire des analyses pertinentes et contribuer à une information plus transparente.

---

[1] What is OSINT (Open-Source Intelligence?) | SANS Institute
https://www.sans.org/blog/what-is-open-source-intelligence

[2] [7] What Is Open Source Intelligence (OSINT)?
https://www.recordedfuture.com/blog/open-source-intelligence-definition

[3] Verification-Handbook-1.pdf
https://s3.eu-central-1.amazonaws.com/datajournalismcom/handbooks/Verification-Handbook-1.pdf

[4] [5] The Historical Use of OSINT Through The Centuries | IMSL
https://www.intelmsl.com/osint-history/

[6] Tales from the History of OSINT: Foreign Broadcast Information Services
https://verosint.com/post/tales-from-the-history-of-osint-foreign-broadcast-information-services

[8] Using Open-Source Intelligence (OSINT) in Journalism | Al Jazeera Media Institute
https://institute.aljazeera.net/en/ajr/article/2159

[9] [17] Developing the Berkeley Protocol - Berkeley Human Rights Center
https://humanrights.berkeley.edu/projects/developing-the-berkeley-protocol-on-digital-open-source-investigations/

[10] [11] [12] What is OSINT Open Source Intelligence? | Trend Micro (UK)
https://www.trendmicro.com/en_gb/what-is/threat-detection/open-source-intelligence-osint.html

[13] The Journey from Open-Source Information to OSINT | GDIT
https://www.gdit.com/perspectives/latest/the-journey-from-open-source-information-to-osint/

[14] [15] [16] Using open-source intelligence to investigate human trafficking and migrant smuggling
https://www.unodc.org/unodc/frontpage/2025/March/using-open-source-intelligence-to-investigate-human-trafficking-and-migrant-smuggling.html

[18] [19] Congress wants the Army to start collecting more open-source intelligence - Defense One
https://www.defenseone.com/policy/2025/02/congress-wants-army-start-collecting-more-open-source-intelligence/402934/

[20] [21] [40] New free eLearning course on open-source intelligence (OSINT) | Basel Institute on Governance
https://baselgovernance.org/news/new-free-elearning-course-open-source-intelligence-osint

[22] [23] Free Course | Introduction To OSINT | BTJA
https://www.securityblue.team/courses/introduction-to-osint

[24] [25] OSINT | Basel Institute LEARN
https://learn.baselgovernance.org/enrol/index.php

[26] [27] OSINT Beginners Course
https://training.kapsuungroup.com/courses/osint-beginners-course

[28] 100+ OSINT (Open Source Intelligence) Online Courses for 2025 | Explore Free Courses & Certifications | Class Central
https://www.classcentral.com/subject/osint

[29] [30] [31] [32] [33] [36] [39] Top 5 Practical OSINT Books, 2025 | Blog | Social Links
https://blog.sociallinks.io/top-5-books-for-sharpening-your-osint-skills-in-2025/

[34] [35] Best OSINT Books: Expert Picks & Free Downloads
https://www.osintteam.com/books/

[37] Best Ways To Learn OSINT In 2025
https://www.martinpi.com/best-ways-to-learn-osint-in-2025/

[38] OSINT Framework
https://osintframework.com/