Résumé de la Journée OSINT 2025

Ouverture et présentation générale

La journée OSINT a débuté à 9h20 avec une présentation par le directeur du master Géopolitique et GEOINT, qui a posé le cadre académique et stratégique de cette journée dédiée aux différents usages professionnels de la recherche en sources ouvertes.

Intervention de Ludovic HUTH – Directeur du Campus OSINT

Ludovic Huth, directeur du Campus OSINT (DGA), a ensuite officiellement parrainé la journée et a présenté la vision du ministère des Armées sur l'OSINT. Pour la DGA, l'OSINT recouvre toutes les informations accessibles librement et présentant un intérêt pour les forces armées. Cela inclut la veille technologique, le suivi des réseaux sociaux, le GEOINT (géolocalisation d'informations), ou encore la market intelligence. Il a présenté la création récente du Campus OSINT en juillet 2024, officiellement lancé en octobre, avec une double mission :

1. Fédérer l'ensemble de l'écosystème OSINT rattaché au ministère des Armées, incluant institutions, chercheurs, entreprises et praticiens.
2. Soutenir activement l'intelligence économique au bénéfice de la Base industrielle et technologique de défense (BITD), en renforçant les dispositifs de sécurité économique nationale.

Cellule d'intelligence stratégique – Safran

Les intervenants Jordan Jeambenoit et Raphaël Zwein, responsables au sein de la cellule d'intelligence stratégique de Safran, ont détaillé les pratiques de veille dans leur entreprise. Safran, acteur majeur de l'industrie aéronautique, spatiale et de défense, fait de l'OSINT un levier essentiel de compréhension des marchés et de la concurrence. Leur cellule s'organise autour de quatre axes :

- Un processus d'enquête structuré pour organiser et fiabiliser les recherches.
- L'exploitation de différentes catégories de données (publiques, brutes ou achetées).
- Une veille concurrentielle ciblée sur les évolutions technologiques et industrielles.
- Un strict respect du cadre légal et éthique en matière de collecte et de traitement des données.

Ils ont insisté sur la non-magie de l'OSINT : l'information n'est ni gratuite, ni systématiquement accessible, ni toujours rentable. La direction de la stratégie et de l'innovation est leur principal commanditaire, et les données extérieures sont essentielles pour guider les décisions. Ils constatent cependant une forte dépendance à l'OSINT, dans un contexte marqué par trois défis majeurs :

- Une attrition des données directes : les entreprises contrôlent mieux leur communication, rendant plus difficile l'accès à des informations sensibles.
- Une baisse de la valeur des données disponibles : prolifération des contenus IA, baisse de la qualité journalistique, difficulté de traitement pertinent.
- Un coût croissant d'accès et d'outillage : industrialiser la collecte devient onéreux.

Pour répondre à cela, Safran développe une culture OSINT rigoureuse, visant à former des binômes compétents et critiques, à automatiser les tâches répétitives, et à standardiser les livrables. L'IA joue un

rôle croissant dans l'optimisation de la veille (ex. : Newscore, Craft My Deck), bien que sa valeur ajoutée réelle réside surtout dans le soutien à l'analyse, et non dans l'analyse elle-même.

Red Team et OSINT – ATSecurity

Alexandre Triffault (expert en intrusion physique) et Lisa Beasse (spécialiste junior en OSINT) ont présenté les méthodes de la Red Team d'ATSecurity. Leur mission est de tester la robustesse de la sécurité d'une organisation en simulant des attaques réalistes, notamment par intrusion physique.

Deux types d'audit ont été présentés :

- L'audit en boîte blanche : basé sur un échange avec le client, utile mais peu représentatif des vulnérabilités concrètes d'usage.
- L'audit en boîte noire : sans information préalable, simulation complète d'une intrusion avec repérage sur site, HUMINT et pénétration physique.

L'OSINT est ici décisif. Il permet d'identifier les points d'entrée (portes de service, badges, ascenseurs, parkings), de repérer les prestataires (cafetiers, techniciens) pour se faire passer pour eux, ou encore de reconstituer des plans de bâtiments via appels d'offres publics. Ils ont montré comment, avec des photos et des vidéos trouvées en ligne (ex. : bureaux de Leboncoin), ils pouvaient reconstituer les badges, les uniformes ou repérer les dispositifs de sécurité. L'OSINT est également utilisé en rétro-ingénierie pour comprendre les techniques employées lors de véritables intrusions criminelles.

Due Diligence – Agency E

Emeline, analyste au sein d'Agency E, a présenté les méthodes d'enquête OSINT appliquées à la due diligence. Celle-ci vise à vérifier la solidité, la réputation ou les risques associés à un futur partenaire économique (entreprise ou individu). En France, elle est encadrée par la loi Sapin II et la loi n°2017-399 du 27 mars 2017.

La méthode repose sur la création d'une carte mentale, utilisée comme feuille de route pour croiser les sources, identifier les points de vigilance et structurer l'enquête. Celle-ci peut comporter plusieurs niveaux : vérification de CV, recherche sur les dirigeants, identification de liens financiers, analyse de réputation, etc. Emeline a présenté plusieurs cas concrets :

- Un investisseur offshore difficilement traçable, nécessitant une enquête terrain.
- Un candidat d'origine russe dont le refus de transparence sur son parcours a éveillé des soupçons.
- Un sous-traitant dont les activités ont mené à une action judiciaire pour concurrence déloyale.

Renseignement criminel et police judiciaire – Gendarmerie nationale

Le colonel Jérôme Barlatier a présenté une distinction claire entre deux métiers : le renseignement criminel et l'enquête judiciaire. Le premier est proactif, global, stratégique. Il vise à comprendre pour anticiper et entraver. Le second est réactif, fondé sur la preuve, et vise à constater, identifier, arrêter et juger.

L'OSINT est utilisé à toutes les étapes, depuis la veille et l'alerte jusqu'à la contextualisation environnementale. Plusieurs exemples ont été donnés :

- L'exploitation d'annonces de prostitution en ligne à l'occasion des JO pour repérer des réseaux.
- L'analyse des réseaux de cyberarnaques (ex. : les « brouteurs »).

- La détection de dépôts sauvages de déchets grâce à la géolocalisation satellite.
- L'analyse culturelle embarquée dans des enquêtes sensibles (ex. : influence des forums type creepypasta dans des cas de parricide).

L'enquête judiciaire nécessite l'usage loyal et traçable de l'OSINT : identification et localisation de suspects, gel des données numériques, exploitation des réseaux sociaux. Elle doit respecter la loi, garantir la reproductibilité, et se prémunir contre les dérives type leaks ou vigilantisme.

OSINT et journalisme d'investigation – RFI

Grégory Genevrier et Olivier Fourt ont présenté les travaux de la cellule OSINT d'Infovérif à RFI. Créée en 2023, cette cellule produit du contenu pour la radio et le web, notamment la chronique "Les dessous de l'infox". L'OSINT journalistique permet de documenter des terrains inaccessibles, d'analyser les campagnes de désinformation, et de vérifier les sources en toute transparence.

Les outils utilisés incluent des moteurs de recherche inversée (Yandex, PimEyes), des outils de géolocalisation (Mapillary, Google Earth), et des bases satellites (Copernicus, Maxar). Un exemple marquant : une vidéo filmée à Bamako présentée comme un convoi humanitaire révélait en fait un transfert d'armement via la Guinée. Les journalistes ont insisté sur les contraintes de leur métier : respect de la charte déontologique, manque de financement, temporisation nécessaire.

Table ronde – Intelligence artificielle et OSINT

La table ronde a permis d'explorer les apports et limites de l'IA dans les pratiques de veille et d'OSINT, à travers les regards croisés de praticiens issus de la veille institutionnelle, de start-ups et du gouvernement.

- **Rôle actuel de l'IA** : L'IA est utilisée pour automatiser la collecte, la synthèse et le tri de grandes masses d'informations. Elle soutient les analystes dans l'identification de documents pertinents et dans l'agrégation thématique. Certains outils permettent la modélisation de persona ou de scénarios pour tester des hypothèses analytiques. D'autres facilitent la génération de livrables (ex. : synthèse audio ou vidéo).
- **Enjeux critiques** : La confiance dans l'IA passe par la transparence des modèles utilisés, notamment sur la manière dont les informations sont hiérarchisées. La question de la souveraineté numérique et de l'hébergement local des données est également centrale. L'IA doit être formée sur des corpus adaptés à ses usages, et ne doit pas être utilisée à l'aveugle : les prompts doivent être pertinents, les résultats vérifiés.
- **Exemples concrets** : À La Poste, l'IA permet de lire plusieurs centaines d'articles, d'identifier ceux pertinents, puis de transmettre une synthèse pour traitement humain. En veille concurrentielle, elle peut repérer des signaux comme l'entrée de nouveaux acteurs dans le secteur spatial. Toutefois, les articles rédigés par IA sont globalement moins lus et consultés que ceux écrits par des journalistes.
- **Signaux faibles** : Les modèles IA ne sont pas encore capables de détecter seuls les signaux faibles. Ils sont performants dans l'extraction de tendances dominantes mais peinent à capter des signaux discrets et peu probables. En revanche, ils peuvent valider ou invalider des intuitions humaines.
- **Prospective** : D'ici 10 à 15 ans, l'IA devrait s'inscrire dans des logiques conversationnelles plus évoluées. Les analystes travailleront avec elle comme avec un collaborateur virtuel. Les formats

des livrables évolueront (audio, vidéo, livrables interactifs), et l'enjeu sera de créer des processus augmentant les capacités humaines sans les remplacer. Les questionnements sur l'impact écologique, social et éthique de l'IA restent entiers.