

« LIBERTÉ ET PROSPECTIVE » Le Think Tank

"Il n'est point de bonheur sans liberté, ni de liberté sans courage." Périclès

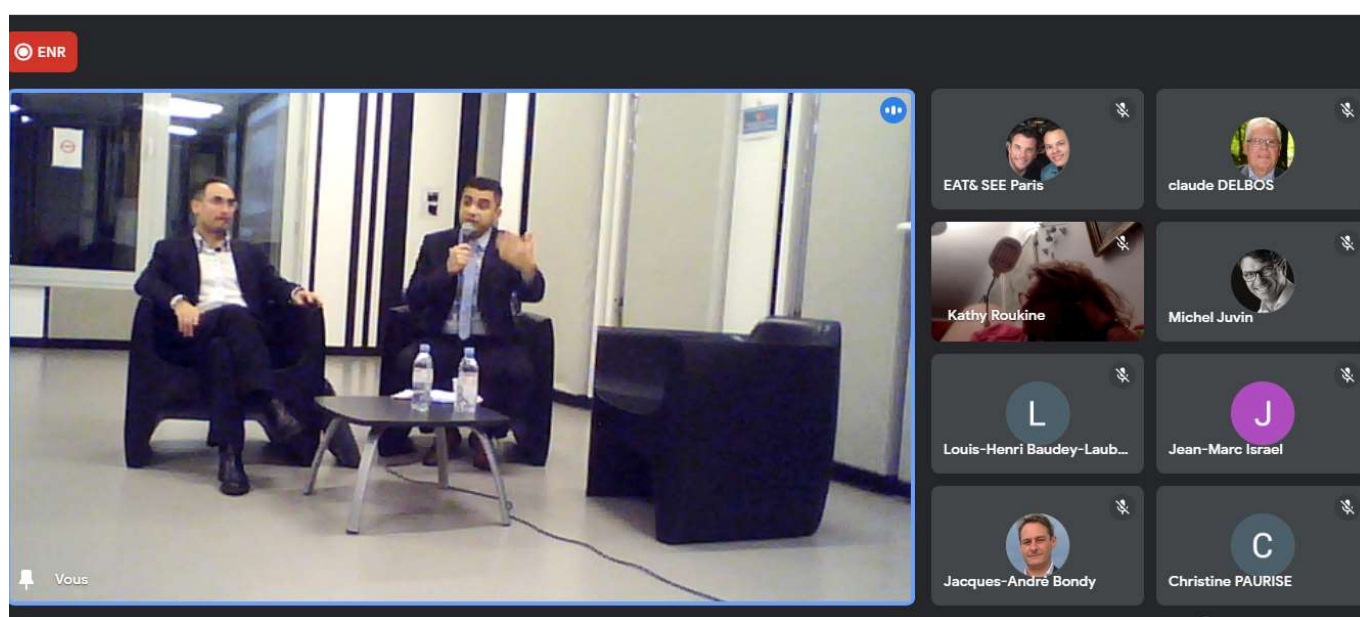
Qu'est-ce que l'OSINT ?

Open Source Intelligence ou Information en Source Ouverte

David G. DENIEL, Directeur du numérique du Think Tank

Laurent GOYCHMAN, Responsable de projets innovants et de l'atelier Intelligence Économique du Think Tank

enregistrement lien : <https://youtu.be/gaRcblU1OUU>



Le 25 Janvier 2022, s'est tenu à la Maison des Associations du 8e Arrondissement à Paris, une conférence d'introduction intitulée « **Qu'est-ce-que l'Osint ?** » avec deux intervenants **David Guillaume Deniel** et **Laurent Goychman**, sous l'égide de la Présidente **Henriette Caux** du Think Tank Liberté et Prospective. Cette conférence d'une heure, donne la parole deux fois vingt minutes à deux experts qui vont explorer deux voies de l'Osint (Open Source Intelligence Tools), son Evolution Militaire puis Civile avec David Guillaume Deniel et son aspect entrepreneurial avec Laurent Goychman.

David Guillaume Deniel prend en premier la parole pour évoquer les origines de l'Osint, que l'on peut traduire et identifier comme les **outils développés pour recueillir des renseignements à partir de sources d'information publiques**. Ce concept au départ regroupait aussi bien l'analyse des Presses Écrites Nationales étrangères, que l'analyse des émissions de radio ou les simples discussions de comptoir des obscures tavernes de matelots. Il faudra attendre la fin de la seconde guerre mondiale pour que la CIA développe son

département Foreign Broadcast Information Service, puis le mue en 2005 en OPS - Open Source Center pour qu'apparaisse le terme Osint. Naturellement, le but de ces 2 départements était d'agrèger toutes les sources d'informations disponibles et venant des pays étrangers, collectées à l'origine par leur fameux prédécesseur l'OSS - Office Strategic Services

Très rapidement avec l'apparition des **nouvelles technologies, et encore plus avec internet et les réseaux sociaux**, tous les **services de renseignement** se sont aperçus de la démultiplication des capteurs d'informations, et de la réduction possibles des coûts d'obtention des informations liée à la disparation des interventions physiques sur sites. De **multiple mises à disposition d'informations, ainsi que le nombre croissant de techniques d'analyses** devenaient possibles. Avec un simple ordinateur, une connexion internet et des abonnements à des réseaux sociaux, comme Facebook, Twitter, Instagram... Des myriades d'informations étaient désormais disponibles à portée de clics.

La deuxième évolution est que **pour atteindre et exploiter ces sources d'information disponibles, les agences de renseignement ont commencé à développer des outils en internes de recueil et d'analyse**. Ces outils, qui restent toujours aussi puissants aujourd'hui, sont peu intuitifs et fonctionnels, et restent souvent utilisés par des spécialistes ou des initiés. C'est la troisième évolution qui va permettre d'améliorer, et l'accès aux multiples bases de données en simultanément, et les interfaces utilisation / modélisations, tout en permettant l'interfaçage avec d'autres sources de renseignements en temps réels. Tout cela va créer un nouveau et véritable marché, qui donnera aux entreprises la possibilité de développer des solutions et des logiciels innovants à destination des Etats. Des sociétés connues comme Palentir vont pouvoir alors proposer des solutions associant Interface Intelligente, Business Intelligence & Intelligence Artificielle pour aller au-delà de l'internet, et incorporer des données comme celles des satellites à côté du renseignement humain et de la dimension Temps réel.

Mais comme pour toutes les avancées technologiques, **de nombreuses sociétés vont rapidement ouvrir au grand public une partie de ce savoir-faire**, en proposant des versions gratuites ou payantes de leurs outils, tout en limitant l'accès aux données. Cette **transition Classique d'une innovation Militaire au monde Civil**, va malheureusement permettre de plus en plus à monsieur tout le monde d'espionner son voisin. C'est là où le bât commence à blesser et que les problèmes surgissent, car les données sont multiples, nombreuses et disponibles dans tout cet environnement numérique.

En effet, volontairement ou involontairement, nous laissons des **traces numériques** lors de nos navigations sur internet, et cela, quelle que soit nos activités. Même sur des sites sécurisés, ces traces peuvent faire l'objet de vols pendant plusieurs jours ou plusieurs mois **par des « hackers », et à l'insu de l'entreprise, et de l'hébergeur et de l'utilisateur**. Ces données privées captées et revendues plusieurs fois sur le darknet pour quelques centaines d'euro, deviennent à leurs tours des données en libre d'accès. C'est cela le premier risque.

Le Second risque est que certaines sociétés qui ont compris **la lucrativité de ce nouveau marché**, donnent accès pour quelques dizaines d'euros, et à des outils d'une grande facilité d'utilisation, et l'accès à de nombreuses sources d'information dites publiques. Ces outils permettent alors, à n'importe qui d'avoir le pouvoir d'espionner qui il souhaite. Ce n'importe qui peut donc faire n'importe quoi, comme un usage irréfléchi des résultats et des analyses qu'il a obtenu.

Pour le futur de l'Osint ? nous savons déjà qu'il s'agit du WebInt, c'est-à-dire l'association des collectes de données passives de l'Osint avec les interactions en temps réelles des utilisateurs sur les réseaux, comme dans les forums par exemple.

Laurent Goychman confirme les derniers éléments soulevés par David Guillaume et souligne les deux effets pervers de cette situation, à savoir la création d'une situation et d'un espace confus, interlope où circule des informations qui par définition ne devraient pas être là, ni être accessibles et consultables.

Il rappelle toutefois que **les sources ouvertes existent depuis longtemps** (presse écrite, puis médias classiques, littérature « grise » constituée des rapports scientifiques et professionnels), mais ce n'est qu'au 19e siècle, avec l'essor du monde bancaire « mondialisé » (exemple des cinq frères Rothschild, implantés chacun dans une grande capitale européenne) que ces sources ont pris une autre dimension. Au début du 20e siècle, les schémas directeurs étaient similaires à ceux d'aujourd'hui. Les grandes capitales étaient connectées, et les moyens de communications rapides présents. Ce qui permettait aux acteurs économiques d'observer l'environnement global, et de réaliser une analyse sous le cadre PESTEL (acronyme de politique, économique, sociologique, technologique, environnemental et légal) afin d'anticiper les actions et réaliser les bons investissements au bon moment.

Avant Internet, la presse, les médias, la radio, ainsi que les salons professionnels jouaient un rôle essentiel, ce rôle est aujourd'hui partagé, mais n'a pas disparu. Il est toujours analysé par les services de renseignements, mais aussi par les organismes de veille, les entreprises.

On peut faire une analogie entre les **données personnelles** que l'on retrouve dans le **dark web** et les **données économiques et financières des entreprises** qui fuient plus ou moins volontairement et qui sont, pour le **secteur bancaire**, notamment américain (pilote par l'Administration U.S.) une raison particulière d'intervenir.

En effet, depuis **l'affaire Enron en 2001**, qui a laissé dans l'inconscient américain de nombreuses traces, la nouvelle législation et les nouvelles normes juridiques et comptables américaines édictées, notamment Sarbanes-Oxley, **obligent les entreprises à rendre public nombre d'informations, afin de limiter les délits d'initiés à leur profit**. L'État américain a étendu cette situation pour accroître son influence et imposer ses règles, en les exportant hors de leurs frontières, (apparition d'une **extra-territorialité du droit US**), en interdisant à des entreprises étrangères de commercer avec des pays avec qui elle est en conflit, sans distinguer la nature de ses échanges. Cette obligation, ce devoir peut conduire l'entreprise à de lourdes **sanctions financières**. Des entreprises comme **BNP Paribas** (investissement en Iran) ou Airbus en ont fait les frais. Tous les moments de la vie de l'entreprise peuvent alors devenir des périodes sensibles, particulièrement les fusion-acquisitions, qui sont des moments critiques où les risques de fuites peuvent être sources de préjudices.

Si un employé, et dans un groupe il y en a beaucoup, par une simple veille Osint, mets à jour une fuite d'informations relatives à une Fusion-Acquisition, la banque américaine va alors revoir à la hausse le montant de son pourcentage de sa commission. Cette ruse permet donc aux cabinets d'audit américains présents sur toutes les places boursières mondiales, d'auditer les entreprises et de réaliser un juteux marché de « Due intelligence ».

Cette concurrence du droit américain sur le sol européen est très difficile à contrer au niveau européen. L'Europe sur ce point apporte peu d'aide et de soutien. Il suffit de peu de chose pour attirer l'attention des autorités américaines. Ainsi une PME française, pour peu qu'elle soit innovante, peut entrer dans le viseur des Etats-Unis. Et malheureusement, l'utilisation d'outils de partage / stockage des données (fournis par les **GAFAM (Google, Apple, Facebook et Amazon, Microsoft)**) donne aux USA l'occasion de pouvoir regarder de très près ces innovations. Pour Laurent Goychman, nous sous-estimons les outils que nous utilisons par commodité (ou peur de la nouveauté, même locale, également connu sous l'appellation « syndrome du DSI », qui ne fait confiance qu'aux fournisseurs de solutions leader du marché) Certes, ils sont puissants et bien conçus, mais nous n'en avons pas la maîtrise et nous ne savons pas où circule l'information. Ainsi, la création d'un cloud souverain (véritable) est une nécessité, un enjeu majeur pour retrouver une souveraineté numérique.

Thierry Breton ancien PdG d'Atos et actuel Commissaire Européen y œuvre actuellement.

Pour finir sur une note positive, on peut dire que **l'intelligence économique est un enjeu de politique publique, c'est à dire l'affaire de tous.**

Biographies :

David Guillaume DENIEL-AZOULAY a commencé sa carrière chez **KPMG France** en 2001, comme Responsable des Innovations IT Business. Puis il a travaillé dans des sociétés internationales de taille Européennes ou Internationales en Europe, en Amérique du Nord et au Moyen Orient. Depuis 2015, Il s'est spécialisé dans la **CyberSecurite**. Ancien élève de l'Institut Supérieur de Gestion à Paris et du Manhattan Institute of Mana.

<https://www.youtube.com/watch?v=yX3GTRRXu6s>gement New-York.

<https://telquel.ma/podcasts/lescan/2021/07/23/nso-ou-la-democratisation-de-lespionnage?fbrefresh=5>

Laurent Goychman Responsable de projets innovants et de l'atelier Intelligence Économique du Think Tank. A l'issue de son service militaire dans les troupes de marine (Fréjus puis Djibouti), il reprend des études d'Ingénieur-Juriste en Environnement. Il démarre dans le conseil en financement de l'innovation, puis évolue vers des collectivités territoriales, en développement économique / accompagnement de créateurs, avec un focus sur l'innovation et l'intelligence économique. Il est titulaire d'un Executive MBA sur le campus HEC.