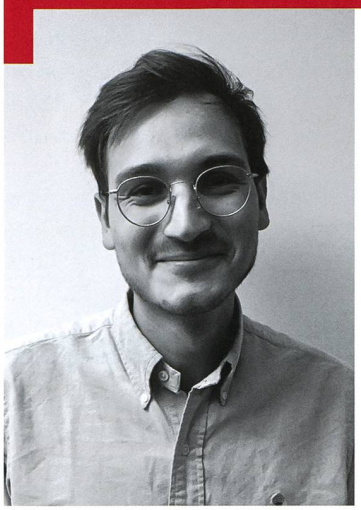
**Zeitschrift:** Revue Militaire Suisse
**Band:** - (2020)
**Heft:** 6

**Artikel:** Les défis du renseignement d'origine de sources ouvertes pendant la pandémie du coronavirus
**Autor:** Cordey, Sean / Baezner, Marie
**DOI:** https://doi.org/10.5169/seals-913932



Pendant la pandémie, les informations transmisent par les organes nationaux et internationaux n'ont pas toujours été vérifiables ou valides.

*Renseignement*

## Les défis du renseignement d'origine de sources ouvertes pendant la pandémie du coronavirus

**Sean Cordey*, Marie Baezner ****
* Chercheur au Cyber Defense Project, Center for Security Studies (CSS), EPFZ
** Collaboratrice scientifique, cyberdefence, Base d'aide au commandement (BAC)

Tout comme la société en général, la pandémie du coronavirus a aussi bouleversé la communauté du renseignement occidental. Elle a généré une nouvelle demande pour ce que beaucoup nomment « le renseignement de santé publique » – un mandat que beaucoup d'agences de sécurité et de renseignements n'avaient, en réalité, jusqu'à là, pas ou peu considéré comme part de leur mandat (hormis le Med Intel).[1] La mission du renseignement est ainsi devenue double: surveiller et analyser l'évolution, la transmission et les implications du virus (à l'interne et à l'externe) tout en luttant contre les menaces « traditionnelles » qui se retrouve amplifiées comme la dés/mal-information, la fraude ou l'ingérence étrangère. Quant à cette première mission, les services de renseignements doivent user de leurs différents outils de collections, comme l'interception de signaux électromagnétiques (SIGINT), les images satellites (IMINT), les contacts humains (HUMINT), ou encore des informations de sources ouvertes (OSINT).

Dans le contexte du « renseignement de santé publique », les sources ouvertes jouent un rôle essentiel, notamment concernant des systèmes d'alertes, de détection et de suivi des pandémies.[2] Son accessibilité en fait également un outil de choix au-delà du cadre du renseignement. Bien qu'utilisé depuis des années, l'OSINT se retrouve toutefois (re)valorisé depuis plusieurs mois. Dès lors, se pose la question suivante : quels défis et implications pour l'OSINT a présenté la pandémie du coronavirus? Pour y répondre, cet article introduit dans une première partie l'OSINT avant d'élaborer dans une deuxième partie deux des défis majeurs pour l'OSINT en temps de pandémie avant de conclure en expliquant certaines implications quant à sa (re)valorisation.

### Présentation de l'OSINT

Avant d'élaborer sur les défis et implications de la pandémie sur le renseignement de sources ouvertes, il convient tout d'abord de définir et replacer ce qu'est le Renseignement d'Origine Sources Ouvertes (ROSO) – plus communément dénommé « Open Source Intelligence » (OSINT). Concept Americain, on entend par OSINT la collecte, l'analyse et diffusion d'information obtenue à travers des sources d'information publiques (payantes ou gratuites). Du fait de la digitalisation croissante de la société et de la multiplication des médias en tous genres, ces dites sources d'information peuvent être d'une grande variété: télévision, journaux papiers, blogs, sites internet, réseaux sociaux, metadata, imagerie satellite, publications académiques, gouvernementales ou encore commerciales. A l'encontre de la recherche classique, qui a pour but l'acquisition de connaissances, l'OSINT applique des processus et techniques de renseignements dans les buts de recherche d'information dans le cadre d'une tâche spécifique (ex. surveillance journalière des cas de coronavirus), de prévenir des menaces et de supporter la prise de décision.

Les services de renseignements – parfois spécialisé comme l'Open Source Center américain – en sont parmi les plus grands utilisateurs, que ce soit pour des motifs de sécurité nationale, de lutte contre le terrorisme et le (cyber)crime ou de renseignement extérieur. L'OSINT n'est pas réservé qu'à ces derniers et pour beaucoup d'autres services gouvernementaux, c'est souvent le seul moyen d'obtenir des informations.[3] Les autorités policières, par exemple, ont recours à la surveillance automatisée des réseaux

1 Wark., W. (2020, Avril 14). *Pandemic gives security and intelligence community and urgent new mission.* Policy Options. https://policyoptions.irpp.org/magazines/april-2020/pandemic-gives-security-and-intelligence-community-an-urgent-new-mission/

2 Loprespub., (2020, Avril 28). *Le renseignement de sources ouvertes et l'alerte rapide en situation de pandémie.* Bibliothèque du Parlement Canadien. https://notesdelacolline.ca/2020/04/28/le-renseignement-de-sources-ouvertes-et-lalerte-rapide-en-situation-de-pandemie/

3 Center for Security Studies, (Avril 2008). *Open Source Intelligence: nouveau paradigme du renseignement?.* Politique de sécurité : analyses du CSS. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-32-FR.pdf

sociaux ou des programmes de reconnaissances faciales comme *Clearview AI*.[4] Similairement, les organisations internationales comme l'ONU ou la Croix-Rouge utilisent l'OSINT pour soutenir et sauvegarder leurs diverses opérations. Le secteur commercial en est également friand – si ce n'est plus que le secteur public – notamment dans le cadre de l'étude de nouveaux marchés, la surveillance de la concurrence, la planification marketing ou la lutte contre les cyber-risques. On retrouve également toute un écosystème proposant des services d'OSINT pour des tiers (ex. Oxford Analytica ou L'Economist Intelligence Unit). Finalement, l'OSINT est aussi employé comme technique de reconnaissance par des acteurs malicieux, que ce soit des hackers, criminels ou terroristes.

Comparé aux autres moyens de collecte de renseignements, l'OSINT présente un certain nombre d'avantages. Tout d'abord, il ne présente aucun risque réel. De plus, il est généralement moins coûteux, ne nécessitant pas d'équipements sophistiqués (ex. des bases SIGINT ou satellites espions). Les informations accessibles au public sont non seulement faciles d'accès, mais peuvent en outre être recueillies par un cercle d'analystes décentralisés et d'utilisateurs potentiels beaucoup plus grand. A cela s'ajoute le peu de contraintes juridiques et de confidentialité qui encadre la collecte et la diffusion de ces renseignements.

## Pandémie coronavirus : les défis pour l'OSINT

De manière générale, le ROSO doit faire face à de nombreux défis, les plus importants étant : 1) le volume toujours plus croissant de données et d'informations accessibles ainsi que 2) la fiabilité des sources et informations collectées. Bien que la pandémie ait ouvert la voie à de nombreuses applications et opportunités dans le domaine de l'OSINT, elle a également considérablement accentué ces deux défis.

*1) Volume gargantuesque de données et d'information : une question de triage et de pertinence.*

Tout d'abord, le confinement général des populations a eu pour conséquence une augmentation de l'usage des divers solutions et services numériques (ex. réseaux sociaux, programme de téléconférence, journaux en ligne, le cloud, sites de streaming, ...) que ce soit pour des raisons professionnelles, personnelles ou de divertissement. Le résultat a été une véritable hausse de la demande/génération de données. Les statistiques sur l'utilisation de l'internet en témoignent : à la mi-mars 2020, le centre d'échange internet DE-CIX basé à Francfort - le plus important au monde en termes de trafic de données - a signalé une augmentation de 60 % du traffic (4.2 à 6.8 Térabit (Tbit) par secondes) entre mars 2019 et mars 2020, avec un pic 9.1 Tbit à la mi-mars.[5] Ce niveau record est la plus forte augmentation du trafic de données que la société n'ait jamais enregistré. De leurs côtés, les plateformes de médias sociaux ont aussi connu une forte hausse d'utilisation. Facebook, par exemple, a signalé en mars une augmentation de 50 % des messages dans les pays les plus touchés par le virus.[6] Indiquant que les personnes qui se tenaient auparavant à l'écart des médias sociaux se sont progressivement tournées vers ces plateformes pour s'informer et échanger avec leurs proches – une « habitude » qui généralement perdure une fois prise.[7]

En outre, une pléthore d'informations (tous formats compris) sur la crise sanitaire – ex. rapports officiels et commerciaux, nouvelles, livres... – ont été rendu accessibles au public. Cela est dû à la demande croissante de besoin d'informations des populations, qui a résulté sur une communication de crise constante, institutionnalisée et ritualisée (ex. le nombre d'infections, les mesures de confinement ou les listes rouges). Par logique économique, le secteur privé a également répondu à cette demande en mettant à disposition ses services et informations. En effet, compte tenu de la sensationnalisation de la crise, beaucoup de journaux online ont partiellement abaissé leurs « murs de paiement » (paywall) relatifs à la pandémie. Mesures qui viennent s'ajouter aux dynamiques informationnelles et politiques préexistantes comme le cycle d'information constants ou la décentralisation des sources informationnelles. Au-delà des médias, d'autres acteurs économiques, notamment dans le « Big data », le consulting, l'intelligence économique ou sécuritaire ont capitalisé sur la crise pour vendre leurs produits.

La hausse de la demande et génération de données et d'informations ont créé de nombreuses opportunités d'OSINT à des fins de traçage de la pandémie. Parmi les usages, on y retrouve par exemple, en mars, l'analyse du soudain ralentissement de l'Internet Malaysien qui a laissé entendre une situation sur place pire que les 129 cas alors annoncés.[8] De même que la surveillance d'Internet en Chine tout au long de la pandémie a montré comment les usines industrielles des régions les plus touchées se sont arrêtées pendant l'épidémie avant de reprendre, donnant de cruciales informations sur la situation sur place. Ou encore, les données de TomTom sur le trafic routier de diverses villes chinoises et italiennes ont servi à comprendre comment elles étaient affectées par les quarantaines et les restrictions de mouvement.

4 A noter que les abus sont nombreux et que les techniques ne sont pas toujours au point. Pour rappel, les émeutes de 2015 à Baltimore trouvent entre autre leurs origines dans des messages sur les réseaux sociaux mal interprétés par les forces de l'ordre.

5 DE-CIX, (2020, Mars 11). *Highest jump ever: DE-CIX Frankfurt reaches 9.1 Tbps.* https://www.de-cix.net/%20de/news-events/news/de-cix-frankfurt-reaches-9-1-tbps.com ; De-CIX., (2020 Septembre 11). *Frankfurt Statistics.* https://www.de-cix.net/en/locations/germany/frankfurt/statistics

6 Schultz, A. & Parikh, J., (2020, Mars 24). *Keeping Our Services Stable and Reliable During the COVID-19 Outbreak.* Facebook. https://about.fb.com/news/2020/03/keeping-our-apps-stable-during-covid-19/

7 Blackdot. (2020). *How Covid-19 will impact the use of OSINT.* Blackdot solutions. https://blackdotsolutions.com/osint-covid-19/

8 Volpicello, G., (2020, Mars 20). *Hidden Data is revealing the true scale of the coronavirus outbreak.* Wired. https://www.wired.co.uk/article/coronavirus-spread-data


La dés/mal-information relatant à la pandémie fut rampante et compliqua l'évaluation des sources.

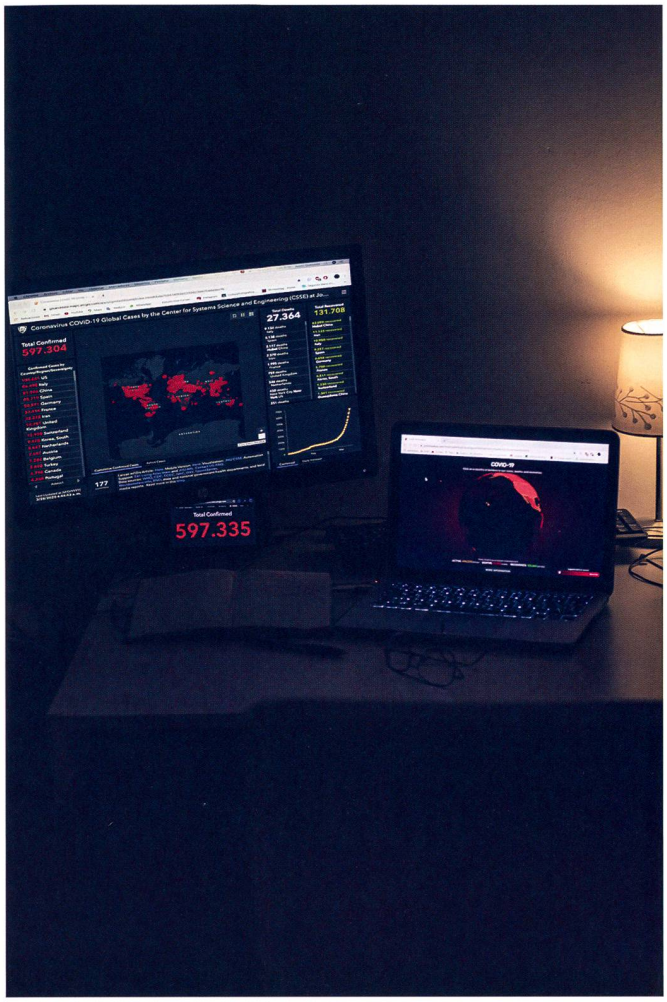
Malgré ces bienfaits, l'explosion et le trop-plein de données et d'informations est également un des défis majeurs pour l'OSINT. En effet, selon Travis Wright, aujourd'hui « *les dirigeants et les organisations ne cherchent plus des aiguilles dans les meules de foin, ils cherchent des aiguilles spécifiques dans des montagnes d'autres aiguilles* ».[9] En effet, la collecte de l'OSINT produit et brasse une grande quantité de données et d'informations qui doivent être fastidieusement triées, filtrées et analysées – à temps – pour être considérées comme utiles et pertinentes. Il existe de nombreux outils automatisés à cette fin, et de nombreux gouvernements et entreprises ont développé leur propre ensemble d'outils et de techniques d'intelligence artificielle pour filtrer les données collectées. Mais de telles informations ne peuvent souvent être vérifiées et questionnées qu'avec des outils de renseignement traditionnels et la « touche humaine ». En effet, il est souvent nécessaire de visualiser et comparer avec certaines données classifiées les résultats des outils automatisés pour s'assurer de leur fiabilité et de leur pertinence – opération chronophage et qui nécessite des ressources humaines. Ce processus a été d'autant plus compliqué lors de cette pandémie, car beaucoup de services de renseignements ont été contraints à une importante réorganisation pour éviter de propager la maladie dans leurs rangs, impliquant parfois une perte d'accès à certains serveurs ou contacts humains.

*Fiabilité des sources* : dés/mal-information, dépassement des institutions nationales et internationales et processus académique en marge.

Le deuxième défi majeur pour l'OSINT est la fiabilité des sources et la véracité des informations, notamment dans un contexte où 1) la dés/mal-information est rampante, 2) les institutions nationales et internationales sont dépassées ou peu fiables et 3) les processus de création de savoir académique fiable sont minés.

La pandémie a vu l'augmentation massive des volumes de données échangés sur Internet – contenus officiels

9 Wright, T. (2020, Mars 19). *The value of Open Source Intelligence in a Pandemic Environment*. RealClearDefense. https://www.realcleardefense.com/articles/2020/03/19/the_value_of_open_source_intelligence_in_a_pandemic_environment_115131.html




L'anxiété et l'incertitude générale ont contribué à une augmentation de la demande et production de données et d'informations, compliquant le travail des analystes d'OSINT tout en leurs offrants de nouvelles opportunités.

ou officieux, confidentiels ou ouverts, exacts ou faux[10] – générant une « infodémie » dans laquelle de nombreux acteurs tentent d'avancer leurs pions stratégiques, économiques ou politiques. Parmi ces acteurs, on retrouve notamment des états (ex. la Chine, la Russie, l'Iran, Israël mais encore les Etats-Unis) qui ont déployé des stratégies d'influence ambigües, voire agressives pouvant utiliser des informations inexactes ou tronquées afin d'avancer divers intérêts dont : le contrôle du narratif autour de la pandémie (ex. la gestion et origines de la pandémie); la perturbation des efforts adverse de lutte contre la pandémie (ex. en augmentant la panique locale ou en réduisant la confiance dans les institutions); ou encore comme tremplin pour de l'espionnage économique, politique, ou médical – notamment concernant les chiffres d'infections et la recherche sur les vaccins (ex. par le biais de « phishing »). S'ajoute une multitude d'acteurs non-étatiques, comme les cybercriminels, les complotistes ou les groupes politiques extrêmes, qui ont – sciemment ou non – diffusés de fausses informations. Parmi la légion d'exemples, citons la question des traitements (ex. l'hydroxychloroquine ou javel), des mesures d'urgence (ex. l'établissement de la loi martiale en Angleterre ou l'instrumentalisation du confinement pour faire taire les Gilets jaunes) ainsi que des complots (ex. l'invasion de l'Europe par les Etats-Unis – cf. « Defender 2020 »).

Tous ces acteurs ont profité, exploité et parfois contribué à un contexte propice à la multiplication des fausses informations. Un contexte qui se définit notamment par un climat généralisé d'isolement, d'incertitude, d'instabilité et de grande anxiété qui a résulté en une demande croissante d'information. Notons aussi une plus grande dépendance et utilisation des réseaux sociaux pour s'informer – renforcée pendant le confinement ainsi qu'une grande accessibilité et maturité des produits et techniques de « cyber influence » (ex. *bots*, faux comptes...). Tout cela dans un climat international et national parfois délétère, polarisé et divisé qui prête à l'abus et l'ingérence.

En plus de la dés/mal-information rampante, mentionnons que les institutions nationales ou internationales qui dirigeaient l'essentiel des efforts contre la pandémie n'ont pas toujours été en mesure de transmettre des informations valides et vérifiées. A l'échelle nationale, de nombreux pays ont délibérément caché et menti sur la situation réelle dans leur pays (ex. Chine et Iran). Alors que les différentes pratiques (parfois régionales) de collecte et de comptage ont rendu beaucoup de ces données suspectes ou simplement erronées – comme ce fut notamment le cas en Suisse lors du chiffrement des infections dues aux boîtes de nuits.[11] A cela s'ajoute aussi le manque de moyens, de préparation, d'entraînement et de coordination au sein même des états et administrations. Dans le cas de la Suisse, on ne peut que penser aux fameux fax des chiffres journaliers de l'OFSP de mars dernier.[12]

Quant au manque de coordination et de vision, le brigadier Raynald Droz – Chef d'état-major du commandement des Opérations – avançait en mars que : « *la plupart d'entre nous – hormis les membres de notre cellule MedIntel – pensions que cela [la situation sanitaire en Chine] ne nous concernerait pas directement.* »[13] A l'échelle internationale, les informations publiées par certaines institutions intergouvernementales ont également été grandement décriées pour leur manque de précision ou leur arrivée tardive. L'OMS est sans doute l'exemple le plus notable : beaucoup d'experts et d'officiels lui ont

10 *24heures*. (2020, Mars 23). *Covid-19* :un défi aussi pour les services de renseignement. 24 heures. https://www.24heures.ch/monde/covid19-defi-services-renseignement/story/12259636

11 OFSP, (2020, Aout 2). *Rectification: les lieux de contamination sont les contextes familiaux et non les boîtes de nuit.* https://www.bag.admin.ch/bag/fr/home/das-bag/aktuell/news/news-02-08-2020.html

12 RTS info. (2020, Mars 18). *Les annonces de nouveaux cas de coronavirus se font par fax.* RTS. https://www.rts.ch/info/suisse/11175710-les-annonces-de-nouveaux-cas-de-coronavirus-se-font-par-fax.html

13 Chevillot, A., & Roten, N. (2020, Mars 24). *Coronavirus : « Si quelqu'un avait voulu fomenter un acte radical, réfléchi et très efficace, il ne s'y serait pas pris autrement ! »*. Heidi.news. https://www.heidi.news/sante/coronavirus-si-quelqu-un-avait-voulu-fomenter-un-acte-radical-reflechi-et-tres-efficace-il-ne-s-y-serait-pas-pris-autrement

reproché d'être sous l'influence du pouvoir chinois ainsi que son manque de transparence et la gestion de la pandémie.[14] En effet, avant de tardivement déclarer que la pandémie était une « Urgence de santé publique de portée internationale », l'OMS aurait répété sans critiques les informations des autorités chinoises tout en ignorant les avertissements des médecins taïwanais. Ceci, ajouté aux multiples aller-retours concernant la nécessité de porter des masques ou non, a considérablement affecté la crédibilité des informations publiées, donc par ricochet celle des institutions.

Alors que le statut de la science est déjà en train de s'éroder, un dernier élément contribuant à la difficile vérifiabilité des sources ouvertes a été la diffusion généralisée et le recours à des sources académiques souvent problématiques. En effet, de par la nouveauté du sujet d'étude et les fonds considérables qui ont été débloqués pour la recherche, il y a eu une course à la publication et à l'attention, souvent au dépens de la rigueur académique (ex. méthodologie et examen par les pairs) et médicale (ex. aveugle, double aveugle, randomisée) – on pense notamment à ces études sur l'hydroxychloroquine qui n'étaient pas randomisées. Compte tenu d'un processus de recherche académique médical – traditionnellement long – la grande majorité des études qui sont publiées ne sont que des pré-études dont les résultats ne doivent pas toujours être pris pour vrai et doivent encore être vérifiés – une distinction que le grand public ne comprend pas toujours. A cela s'ajoute le fait qu'il existe également un pan de la littérature qui provient de pseudo journaux/revues académiques aux tendances prédatrices.[15] Sous couvert de simili authenticité, ces revues publient – contre une rémunération – toutes sortent d'articles sans aucune forme de test de qualité.

## Conclusion

La pandémie du coronavirus n'a que renforcé l'utilité et la nécessité des services de renseignements de considérer l'OSINT comme une branche à part du renseignement.[16] En effet, l'OSINT complète pleinement d'autres types de renseignements grâce au « cross-intelligence ». Essentiel, il permet de complémenter et affiner la compréhension et la connaissance d'une cible d'intérêt et de son environnement, notamment pour l'analyste.[17] Il peut même parfois compenser – jusqu'à un certain point – certaines autres méthodes de renseignement qui se trouve limitées conjoncturellement (ex. l'HUMINT pendant la période de confinement) ou financièrement.

Dans le cadre de la santé publique, en particulier, l'OSINT s'est révélé avoir un important potentiel, particulièrement concernant les systèmes de suivi, de détection et d'alerte précoce. Pour preuve, depuis quelques mois, de nombreuses initiatives en tous genres ont vu le jour – ex. *l'Epidemic Intelligence from Open Source* (EIOS) de l'OMS – ou ont été relancée – ex. *Global Public Health Intelligence Network* du Canada.[18] Ces initiatives et la (re)valorisation de l'OSINT font suite à la réalisation de certains « manquements » – que certains ont qualifiés de « défaillance/échec de renseignement » bien que beaucoup d'experts au sein des divers services de renseignements et agences spécialisées en signalaient les risques depuis des années. Ces dites « défaillances » sont en train de favoriser – comme aux Etats-Unis après le 11 septembre et la guerre en Irak – un réexamen approfondi de la manière dont les informations sont recueillies, analysées et utilisées dans le cadre de la prise de décision. A cela s'ajoute la volonté de certains gouvernements de développer leurs propres compétences dans le domaine pour ne plus dépendre de l'OMS (qui a perdu en crédibilité) ainsi qu'assurer le suivi stratégique et sécuritaire. A cet effet, ce développement ne fait que s'inscrire dans une plus grande dynamique d'(hyper) sécurisation de plus en plus de domaines de nos sociétés. Dynamique qui fait suite à l'élargissement des menaces sécuritaires – et donc mandat des instances de sécurités – depuis la fin de la guerre froide. Après l'environnement, c'est à présent la santé qui se retrouve à nouveau au centre de l'attention de l'appareil sécuritaire.

Pour conclure, malgré la (re)valorisation apportée par la pandémie, l'OSINT ne doit pas être vue par les services de renseignements comme une solution miracle. L'OSINT fait face à des défis – quantité de données et la véracité/vérifiabilité de celles-ci – difficilement surmontables seuls, particulièrement lorsque les organes de renseignements manquent de ressources et d'expertise dans certains domaines (ex. épidémiologie). Dans ce dernier cas, l'expertise pourrait être d'avantage internalisée ou captée au sein des communautés académiques et scientifiques.[19] Il n'empêche qu'il est critique que les services de renseignement développent leurs capacités et connaissances en matière d'OSINT. Non seulement pour répondre à leur mission qui va encore évoluer, mais aussi pour faire face à la grandissante monétisation et privatisation du secret – et donc une fragilisation du monopole du renseignement et *l'ultima ratio* des Etats – menées par les géant américains et asiatiques de la Tech et du web.[20]

S. C. & M. B.

14 Feldwisch-Drentrup, H. (2020, Avril 2) *How WHO became China's Coronavirus Accomplice.* Foreign Policy. https://foreignpolicy.com/2020/04/02/china-coronavirus-who-health-soft-power/

15 RTS. (2020 Aout 8). *Des revues scientifiques prédatrices qui publient n'importe quoi.* https://www.rts.ch/play/radio/cqfd/audio/des-revues-scientifiques-predatrices-qui-publient-nimporte-quoi--les-mollusques-suisses-la-personnalite-des-insectes?id=11534447

16 Charon, P., & Laurencon, F. (2020). *Les nouveaux enjeux du renseignement.* Le Figaro Enquêtes.

17 *Ibid.*

18 Le Canada est en train de mener un audit pour déterminer les causes de sa fermeture par le gouvernement entre Mai 2019 et Août 2020.

19 Charon, P., & Laurençon, F. (2020). *Les nouveaux enjeux du renseignement.* Le Figaro Enquêtes.

20 *Ibid.*