Open Source Intelligence

OSINT est l'acronyme pour Open Source INTelligence, ou renseignement de sources ouvertes. C'est une discipline qui consiste à collecter des données et des informations en ligne.

L'activité OSINT est utilisée par les enquêteurs mais aussi les journalistes, les professionnels de l'informatique et des affaires de sécurité mondiale, le secteur bancaire, afin de détecter les fraudes potentielles, escroqueries, phishing ou le blanchiment d'argent.

Source
Korii
Antoine Hasday
1er juin 2020

1. Comment les enquêtes open source luttent contre la pédocriminalité

Des Sherlock bénévoles aident Europol à déterminer où et quand des images pédopornographiques ont été prises.

En quelques années, le nombre de contenus pédocriminels identifiés en circulation sur internet a explosé. Comme le relate une enquête du New York Times, le National Center for Missing and Exploited Children recensait à lui seul près de 70 millions de signalements en 2019.

Le problème semble s'être aggravé depuis le début de la pandémie de Covid-19. Selon les services de police, certains contenus évoluent vers des pratiques et des violences de plus en plus extrêmes.

Europol a mis la main sur 14 millions de ces images, mais remonter à leur origine est pour le moins ardu. Pour l'assister dans cette tâche, l'agence européenne de police criminelle a recours au *crowdsourcing,* avec l'opération « Stop Child Abuse – Trace an Object ». Après avoir « censuré » les photos et vidéos, Europol les met en ligne et fait appel au public pour retrouver leur provenance.

1.500 heures de travail

En mars 2018, Carlos Gonzales entend parler de cette initiative sur la BBC et décide de se lancer. Il crée un compte Twitter, observe les techniques utilisées par les autres adeptes d'enquête en sources ouvertes (OSINT), échange avec le milieu et commence à chercher par lui-même, avant de collaborer avec le site d'investigation spécialisé Bellingcat.

« Le soutien apporté à Europol a trois objectifs : aider à secourir les victimes, [éliminer les fausses pistes] *et contribuer à la destruction des photos et vidéos* [pédocriminelles] *»,* indique-t-il au sujet de son engagement.

Le fait que les contenus pédopornographiques continuent à circuler et à être visionnés participe du traumatisme des victimes. Il est donc crucial de faire disparaître des images même anciennes.

Pour des raisons de sécurité, très peu de détails peuvent être donnés sur Carlos. Il est ingénieur de formation –pas journaliste– et il a consacré plus de 1 500 heures de travail bénévole à ce projet.

Pour déterminer l'emplacement et la date d'une photographie à partir de presque rien, l'homme a ses astuces. « *L'identification des images est un processus visuel hautement itératif. Nous améliorons d'abord les images numériquement, pour faire ressortir les plus petits indices. La position du Soleil et l'analyse de la végétation sont utiles pour déterminer le lieu d'origine d'une image,* détaille-t-il.

L'ensemble du processus fonctionne par tâtonnement […] *pour vérifier vos hypothèses. »*

Kalahliya, Ukraine

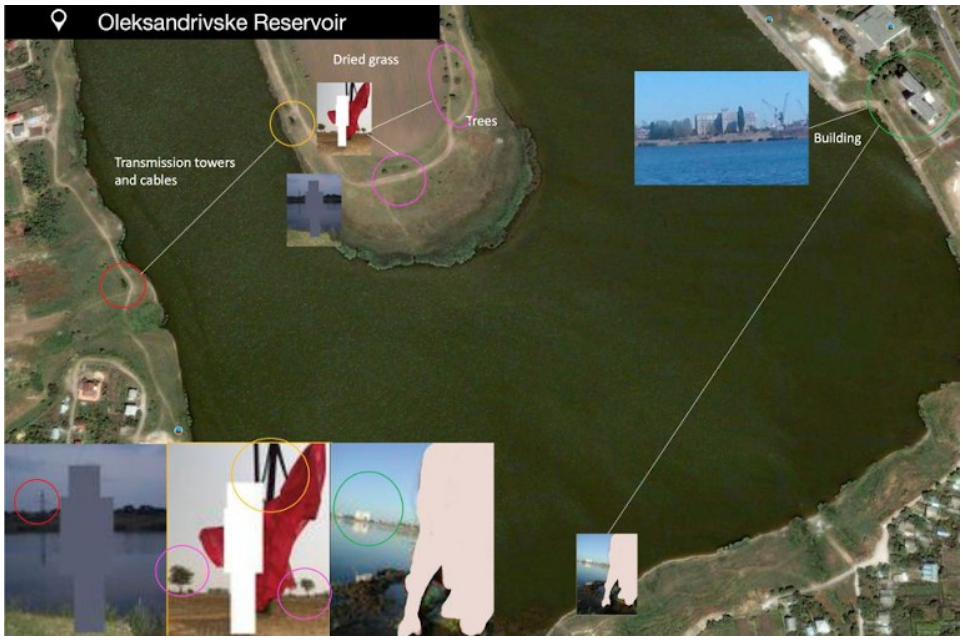
Les premières photos sur lesquelles Carlos Gonzales a travaillé avec d'autres analystes de Bellingcat, qui ont finalement été situées en Ukraine, ont été les plus difficiles à localiser. Un compte rendu détaillé de l'enquête a été publié par Bellingcat, le premier d'une longue série.

« Il y avait un bâtiment d'aspect soviétique à l'arrière-plan, entouré de mauvaises herbes. Nous avons déterminé que ce type de prairies se trouvaient en Ukraine et dans certaines parties de la Russie », simplifie Carlos.

En parallèle, l'équipe se procure un rapport d'enquête mentionnant un trafic d'êtres humains de la Moldavie vers l'Ukraine, en vue de produire des photos et vidéos pédocriminelles dans la région d'Odessa, actif en 2001. Le document comprend des images censurées. « *L'une de ces photos était l'image mise en ligne par Europol. D'autres montraient une église, des ruines...»*

S'en suit un travail de titan pour géolocaliser chacune de ces images dans la région d'Odessa et définir un périmètre, en recherchant des éléments distinctifs disposés dans la même configuration que sur les clichés (bâtiments, ruines, poteaux, forme du littoral...).

Finalement, le village de Kalahliya est identifié. *« L'enquête a nécessité le dévouement de quatre d'entre nous pendant cinq mois ! »,* rapporte Carlos.



Quelques détails peuvent en dire beaucoup sur une image. | Bellingcat / DR

Nosy Kely, Madagascar

La seconde enquête porte sur une photographie unique. Celle-ci montre une plage avec des arbres, sans caractéristiques particulières au premier abord. Mais là aussi, c'est la flore qui va mettre Carlos Gonzales sur la bonne voie.

« J'ai réduit les possibilités en utilisant la recherche inversée de Yandex et les données sur la végétation. Cela m'a amené à enquêter, mètre par mètre, sur la côte ouest de Madagascar à l'aide de Google Earth. Les conifères, les mangroves, les bateaux, les embouchures des rivières et la couleur du sable correspondaient fortement », se souvient-il.

Carlos compile ensuite des vidéos des plages de Madagascar sur YouTube, qu'il visionne les unes après les autres jusqu'à trouver ce qu'il cherche : une plage avec un panneau blanc et trois ombres projetées par des maisons, ainsi qu'un regroupement d'arbres spécifique.

Des recherches plus poussées, comparant par exemple la taille de l'un des arbres sur la photo avec sa hauteur actuelle, permettent de chronolocaliser la photo en 2002.

Une seconde enquête, et quelques indices qui ont mené vers Madagascar. | Bellingcat / DR

Siem Reap, Cambodge

La troisième série de photos semble avoir été prise en Asie Sud-Est, selon Interpol. Carlos Gonzales suit cette piste ; il examine les principales villes de la région sur Google Street View. Une seule possède des poteaux semblables, des arbres similaires et des toits roses : Siem Reap au Cambodge.

L'internaute-enquêteur parcourt kilomètre après kilomètre les principaux axes de la ville sur le service de Google, dans l'espoir de retrouver les éléments présents sur les images. Il utilise également des clichés de la ville mis en ligne sur le site Flickr pour dénicher l'emplacement.

« J'ai finalement retrouvé exactement le même poteau sur l'une routes principales de Siem Reap. L'emplacement du Soleil et des ombres [sur les photos] *m'a aidé à produire un croquis du lieu et à le retrouver »,* précise-t-il.

	N/A	Less Likely	Likely	Most likely	Likely	N/A	N/A
Observation	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**
Satellite image available						Yes	
Concrete Structure	Yes						
Scaffold & Green Netting		Yes	No	No	No	No	No
Front awnings		Yes	Yes	Yes	Yes	Yes	Yes
Windows fitted			Fitting process might have started	Fitted down to ground floor in August	Yes	Yes	Yes
Galvanised Sheets Fencing					Yes		Not anymore
Blue Tarpaulins				Wrong shape seen in April			
Blue tent [16]				Blue area on the same spot observed in October	← Dismantled		
Red parasol observed				Bright	← Faded		
Shack placed on the same spot the blue tent should have been	No	No	No	No	No	Yes	Yes
Young Mango tree at fencing level				Estimated to be at fencing level if growth rate was approx. 1m/year	Above original fence level	←	Above original fence level
Tall trees along the hotel-plot border						Yes	

Pour déterminer la période à laquelle a été prise l'image, Carlos consulte des photos plus ou moins récentes de la zone, où se trouve un hôtel en construction, et compare un certain nombre d'indices visuels. Il parvient à situer la scène autour de 2008.

Des efforts à renforcer

Dans une dernière enquête, Carlos Gonzales se penche sur des photographies en provenance de Russie, du Mexique et de Panama. Les investigations sont bien plus rapides, même si les images russes l'obligent à déployer de nouvelles techniques et à effectuer des recherches internet dans la langue de Pouchkine.

Ce dernier article permet en outre à Carlos de tirer le bilan d'un an de recherches sur le sujet de la pédocriminalité. Selon Europol, une dizaine d'enfants ont pu être secourus grâce à l'ensemble des contributions sur la campagne « Stop Child Abuse – Trace an Object ». Le bénévole estime que ces résultats pourraient être améliorés.

« Il serait utile qu'Europol améliore les descriptions des images pour donner de meilleurs éléments de contexte. De plus, comme Stop Child Abuse repose en grande partie sur [la connaissance du terrain]*, Europol et ses partenaires comme Interpol et les ONG* [devraient] *impliquer davantage de citoyens ordinaires dans le monde,* préconise-t-il*. Les enquêteurs OSINT* [comme nous] *pourraient alors se concentrer sur les affaires les plus difficiles à résoudre. »*

Grâce à l'article sur l'Ukraine, Bellingcat a été nommé dans la catégorie «innovation» à l'European Press Prize. Selon son comité préparatoire, l'enquête est « *simplement supérieure dans sa recherche ».*

Source
letemps.ch
Marie-Amaëlle Touré
1 février 2022

2. Les manœuvres militaires russes épiées sur TikTok

Tandis que les pays occidentaux et la Russie continuent de s'écharper autour de la crise ukrainienne, analystes et enquêteurs tentent d'observer les opérations menées par le Kremlin grâce au réseau social TikTok.

Que prépare Vladimir Poutine ? Tandis que la communauté internationale craint le pire s'agissant de la crise ukrainienne, le réseau social TikTok pourrait apporter quelques éléments de réponse. La tension monte depuis que le Kremlin est accusé d'avoir déployé plus de 100 000 soldats à la frontière ukrainienne en vue d'une possible invasion. La Russie assure ne pas avoir l'intention d'attaquer mais réclame des « garanties » formelles de sécurité, dont l'assurance juridique que l'Ukraine n'entrera jamais dans l'Otan.

Si Vladimir Poutine semble entretenir le flou quant à cette situation, analystes et enquêteurs tentent d'éclaircir les plans du président russe à travers l'application TikTok, ont détaillé plusieurs médias dont NBC NEWS.

« L'application, souvent associée aux tendances de la danse, est maintenant utilisée pour observer une sorte de chorégraphie très différente : les mouvements des forces militaires qui pourraient être sur le point de s'engager dans un nouveau conflit grave sur le sol européen », détaille le média américain.

Chars d'assaut et véhicules blindés

Les vidéos publiées sur le réseau social par des utilisateurs à travers la Russie et la Biélorussie dévoilent des trains chargés de dizaines de chars, de véhicules blindés et d'autres équipements militaires. La semaine passée, un journaliste de la radio américaine Radio Free Europe/Radio Liberty (RFE/RL) avait déjà fait le récit de l'arrivée des soldats russes à la frontière ukrainienne ou en Biélorussie en se fondant sur leurs comptes TikTok.

« Des soldats ont partagé des vidéos TikTok les montrant en train d'aller à la frontière et il y avait des centaines de commentaires comme : 'oh, mon fils va là-bas' ou 'mon fils est sur ce train' ou encore 'mon petit ami est là-bas', a raconté Kiryl Sukhotski, directeur régional de la radio. Alors nous avons commencé à parler à leurs familles qui postaient des commentaires et d'un seul coup nous sommes parvenus à dresser le tableau de ces dizaines de milliers de soldats allant en Biélorussie ou à la frontière ukrainienne, simplement en observant leurs comptes TikTok ».

Moscou nie toute tentative d'invasion

Du printemps arabe au récent assaut du Capitole, les réseaux sociaux se sont érigés en véritables

outils stratégiques de compréhension et de déroulement des conflits. « TikTok, ainsi qu'Instagram sont devenus des plateformes de partage de vidéos à caractère militaire », souligne à CBS NEWS Konrad Muzyka, directeur du groupe Rochan Consulting, spécialisé dans l'analyse de la défense des forces armées russes, ukrainiennes et biélorusses.

L'ampleur du mouvement des équipements en provenance de l'est de la Russie a interpellé l'expert, précise le média américain. Le matériel militaire a parcouru des milliers de kilomètres vers l'ouest. « C'est une chose complexe et sans précédent », a déclaré Konrad Muzyka. […] « Il me semble qu'ils ont apporté, et qu'ils continuent d'apporter des capacités pour réellement mener une opération stratégique contre l'Ukraine. »

De son côté, Moscou continue de nier toute tentative d'invasion. La Russie et les États-Unis se sont déchirés lundi au Conseil de sécurité de l'ONU. Les Occidentaux menacent désormais les oligarques russes de leur faire payer toute escalade militaire. Les États-Unis « continuent à appeler à la diplomatie » pour résoudre la crise autour de l'Ukraine, mais « nous sommes prêts quoi qu'il arrive », a averti lundi le président américain Joe Biden.

Source
letemps.ch
Camille Krafft
17 mars 2022

3. Avec la guerre, les petites mains de l'« Open Source Intelligence » se multiplient

Une communauté d'internautes vérifie et répertorie les informations et les images partagées en ligne. Rencontre avec un ingénieur suisse qui y consacre son temps libre.

Sur l'écran, la photographie d'un bâtiment rouge et blanc éventré avec, à côté, un panneau sur lequel figure une inscription en cyrillique : футбол (football). L'image, postée initialement sur un réseau social, est accompagnée d'un commentaire indiquant qu'elle a été prise dans la région de Tchernihiv, au nord-est de Kiev. L'un des territoires les plus vastes d'Ukraine, 32 000 kilomètres carrés. Pour Benjamin, alias @coupsure, un ingénieur romand actif sur Twitter, la géolocalisation ne prendra que quelques minutes. Google Earth, un peu de flair... Sur l'une des innombrables artères du pays portant le nom du poète Taras Chevtchenko, voici le bâtiment immortalisé par une journée d'été, une journée d'avant la guerre. Il est situé près d'un stade et abritait une librairie, désormais vidée de ses mots.

Nous rencontrons l'ingénieur, qui souhaite préserver son anonymat, dans un café d'une paisible ville suisse de taille moyenne. Casquette et canines juvéniles, Benjamin consacre tout son temps libre à l'Open Source Intelligence (Osint), soit les renseignements obtenus via des sources publiques, comme internet. La guerre en Ukraine, que chacun peut suivre en direct derrière son écran d'ordinateur, génère une quantité d'images, d'informations et de témoignages sans précédent. La communauté Osint tente de vérifier, répertorier, analyser en ligne ce flux continu dans lequel se cachent, bien sûr, des mensonges.

Benjamin procédera ensuite à une *chronolocation*, qui permet de définir à quel moment l'objet a été touché. Une fois confirmées par un enquêteur « senior » de l'ONG londonienne Centre for Information Resilience, les données seront ajoutées à une carte interactive. Ce document visible en ligne répertorie les «incidents» qui ont eu lieu depuis que les troupes russes se sont amassées autour de l'Ukraine : bombardements, échanges de tirs, militaires tués, victimes civiles ou dommages sur des infrastructures. Pour l'ONG, il s'agit d'offrir aux politiques, aux journalistes ou encore à la justice une vision en continu de ce qu'il se passe sur le terrain.

Sources publiques

Touche par touche, ce collectif international et informel, qui fonctionne sur le modèle de Wikipédia, combat l'adage selon lequel la vérité est la première victime de la guerre. Parmi les outils utilisés par Benjamin, il y a des sites de surveillance des avions et des drones, d'autres qui suivent le trafic maritime, ou d'autres encore qui proposent des images satellites gratuites. Sous forme de puzzle, les informations qu'il partage peuvent être complétées. « Par exemple, savoir qui commandait le bataillon qui a tiré peut être utile un jour devant un tribunal. »

Pour l'ingénieur, tout a commencé en 2019, autour du Cachemire. « Ces événements n'étaient pas beaucoup relayés dans la presse. J'ai découvert des comptes Twitter qui faisaient de l'Osint et je me suis lancé. » Partagé en ligne, le fruit de ses recherches est révisé en continu par les autres membres de la communauté. « Si on commet une erreur, on se fait corriger », assure l'internaute, qui a apporté à mesure la preuve de son sérieux. De 4000 abonnés au début de l'année 2021, @coupsure est passé

à 50 000, puis à 160 000 depuis le 24 février. Outre les ONG, le grand public et la justice, son travail peut être utile à certains médias. Benjamin fait partie de ceux qui ont observé les mouvements des troupes russes via les images satellites avant l'invasion. « Le Kremlin annonçait que les troupes se retiraient mais on voyait bien qu'elles se redéployaient. »

Dans la « communauté Osint », on trouve bien sûr Bellingcat, qui a été créé en 2014 par le journaliste britannique Eliot Higgins. Ce média, que les Russes accusent d'être une émanation des services de renseignement occidentaux, s'est fait connaître notamment à travers des enquêtes sur l'abattage d'un avion de ligne dans la région de Donetsk ou l'empoisonnement de l'opposant russe Alexeï Navalny. Autour de cette grosse structure gravitent quantité de professionnels et d'amateurs, comme Benjamin. Alors que ce dernier se concentre plutôt sur la géolocalisation et l'analyse d'images satellites – qu'il paie parfois de sa poche à des sociétés commerciales, par passion –, d'autres ont des centres d'intérêt encore plus spécifiques. À l'image de ce « fan d'Ilyushin Il-76 », qui traque tous les mouvements de l'aéroport d'Addis Abeba. La communauté compte également des spécialistes de la cartographie ou des interceptions radio. N'y a-t-il pas un risque qu'elle soit infiltrée par des comptes diffusant volontairement de fausses informations ? « Je pense qu'on les repérerait très vite », assure Benjamin.

Questions éthiques

Comme d'autres, l'ingénieur se pose quantité de questions éthiques autour de son travail d'Osint : « Je me sens plus proche des Ukrainiens. Est-ce que je peux partager des mouvements de troupes russes sachant que ça les aide ? » Et quid des bataillons abritant des néonazis qui combattent, notamment côté ukrainien ? « En temps de paix, si je peux partager des informations qui les dénoncent, je le ferai. De même, si je vois qu'ils tuent des civils durant le conflit, je relayerai absolument ces données. En attendant, ils se battent, et l'Ukraine a besoin de gens qui se battent. »

Pour l'ONG Human Rights Watch, qui enquête notamment sur les crimes de guerre en Ukraine, utiliser le travail de ces citoyens n'est pas une mauvaise chose, du moment que les informations fournies sont vérifiées. Mais alors que la « communauté Osint » est en plein boom et que de nombreux comptes proposent des outils pour se lancer, certains mettent en garde contre des dérives. « Ce n'est pas un jeu, rappelle le « hacker éthique » toulousain Baptiste Robert. Géolocaliser les troupes peut par exemple donner des informations au camp adverse et lui permettre de faire des frappes ciblées. Un tweet peut avoir des conséquences graves sur le terrain. »

Source
BFM avec TECH & CO
T. L. avec AFP
6 septembre 2022

4. Bellingcat, le pire cauchemar du Kremlin qui documente la guerre en Ukraine

Représentant d'un nouveau mode de journalisme fondé sur l'analyse des données accessibles à tous en ligne, le site d'investigation numérique multiplie les révélations.

Identification des empoisonneurs de Navalny, recensement des crimes de guerre présumés en Ukraine... Le site d'investigation numérique Bellingcat est devenu en huit ans "le pire cauchemar du Kremlin", assure son directeur exécutif, le journaliste Christo Grozev, en lutte contre les lacunes du droit international.

Représentant d'un nouveau mode de journalisme fondé sur l'analyse des données accessibles à tous en ligne -- l'Osint («Open source intelligence» en anglais) -- il s'exprimait lundi à Paris devant un parterre de reporters en devenir ou confirmés, conviés par l'Ecole de journalisme de SciencesPo.

« Nous étions incompétents, nous sommes devenus l'épouvantail », a déclaré le Bulgare pour résumer l'évolution de Bellingcat depuis sa création en juillet 2014 par un blogueur britannique, Eliot Higgins, entouré d'une bandes de "nerds", passionnés d'internet.

Le collectif indépendant, constitué d'apprentis enquêteurs à ses débuts, fait rapidement ses preuves avec son rapport sur le crash du vol MH17, qui a fait 298 morts dans l'est de l'Ukraine, déjà en guerre.

Révélations

Dès novembre 2014, le site accrédite la thèse selon laquelle l'avion a été abattu par un missile russe depuis une zone contrôlée par les séparatistes pro-russes, en retraçant, sur la base de photos, vidéos et documents publics, l'itinéraire d'un lanceur Bouk venu de Koursk en Russie.

Depuis, la plateforme, qui tire son nom d'une fable où des souris s'associent pour accrocher une

clochette au cou d'un chat, multiplie les révélations, notamment sur l'implication présumée des renseignements russes dans les empoisonnements de l'agent double Sergueï Skripal ou de l'opposant Alexeï Navalny.

La Russie, qui a récemment qualifié Bellingcat de "menace", le jugeant "indésirable", n'est "pas notre principal sujet d'enquête", assure à l'AFP Christo Grozev, en charge des enquêtes sur Moscou après une carrière passé dans le milieu des radios privées.

"On a enquêté sur la guerre en Syrie", au Yemen, "sur les violations des droits de l'Homme par (l'office européen de police) Europol, par la Grèce, la Turquie, la Hongrie, sur l'extrême droite aux Etats-Unis, en Ukraine", et généralement sur "les gouvernements qui commettent des crimes parce que personne d'autre n'enquête sur eux".

"La justice internationale a un handicap : elle repose sur l'idée que les gouvernements se préoccupent du bien-être de leurs citoyens", estime Christo Grozev.

La Cour pénale internationale - qui ne peut juger des Etats, seulement des personnes - est par exemple souvent critiquée pour son inefficacité, tandis que les juridictions des pays démocratiques peuvent difficilement collaborer avec des régimes autoritaires pour obtenir des informations.

D'où le travail de fourmi effectué par Bellingcat, qui compte 18 employés à temps plein et une trentaine de collaborateurs à travers le monde.

Coût financier et coût humain

Concernant l'Ukraine, la plateforme s'appuie sur "deux groupes complètement différents et séparés", l'un à visée journalistique, l'autre à visée judiciaire, selon Christo Grozev.

Le premier démine notamment les fausses informations pour déterminer, par exemple, "qui a bombardé" un hôpital ou l'authenticité d'une vidéo montrant un prisonnier de guerre torturé.

L'autre, qui répertorie les crimes de guerre présumés, garde en revanche ses données pour les transmettre à terme à la cour pénale internationale ou aux "onze pays" ayant "lancé leur propres enquêtes sur le principe de la compétence universelle".

Basé au Pays-Bas, Bellingcat est financé à 30 % environ par les formations qu'il dispense à divers professionnels, à l'exclusion désormais de la police, qui "parfois utilise ses méthodes pour violer les droits de l'Homme".

Le reste vient de donateurs privés, en particulier une loterie caritative hollandaise, sensible au travail effectué sur le crash du MH17, parti d'Amsterdam.

Le site n'accepte "plus depuis l'année dernière d'argent provenant de gouvernements" et notamment de la Fondation nationale pour la démocratie (NED), financée par le Congrès américain, insiste Christo Grozev.

La quête acharnée de vérité a aussi un "coût humain", prévient le journaliste, cible de menaces anonymes "deux fois par mois".

Mais "l'adrénaline, le sentiment de faire ce que la justice ou les services secrets ne parviennent pas à faire", comme "les remerciements reçus tous les jours de la part de citoyens russes dans la rue", lui donnent envie de continuer.

Source
Slate.fr
Phénix
16 avril 2023

5. L'OSINT révolutionne le renseignement américain

Grâce à l'Open Source Intelligence, il devient beaucoup plus facile de prévoir ou d'anticiper. Les analystes peuvent affiner leurs hypothèses, les enrichir, les comparer, les confirmer, tout cela à un coût marginal.

En 1999, le hacker américain Éric Raymond publie un essai, *La Cathédrale et le Bazar*, où il expose les principes de l'open source. La Cathédrale correspond au mode « classique » de conception de logiciel, c'est-à-dire une structure organisée, hiérarchisée, compartimentée, avec des armées de programmeurs, de debuggers, des années de développement pour un produit souvent imparfait, voire déjà dépassé par la vitesse d'évolution du marché. Par contraste, le Bazar, c'est la philosophie Linux, c'est-à-dire du code source ouvert, librement partagé et qui permet aux utilisateurs d'y apporter des améliorations et des modifications. C'est la logique de réseau contre la hiérarchie verticalisée.

Or, si tout sépare le monde des geeks anarchistes en baskets et t-shirts criards de celui des espions de Tom Clancy, les mêmes principes de l'open source sont à l'œuvre dans la transformation du renseignement américain : vélocité dans le cycle collecte-traitement-analyse d'informations, décentralisation des sources, explosion quantitative du volume de données traitées, décloisonnement

des disciplines, coopération avec l'extérieur… Pour les services secrets du monde entier, chapelles isolées, hiérarchisées, rétives au changement et méfiantes vis-à-vis de la technologie, on est proche de l'anathème.

Pourtant, comme vient de le montrer le conflit ukrainien, l'Open Source Intelligence ou OSINT (ou encore « renseignement d'origine sources ouvertes » ou ROSO) est au cœur de la révolution qui agite la communauté du renseignement des États-Unis.

Le rôle de l'OSINT à la veille de l'invasion russe

Dès l'automne 2021, les services américains ont acquis la certitude de l'inéluctabilité de la guerre. Cette longueur d'avance sur Poutine a permis aux États-Unis d'accélérer les préparatifs en assistant les Ukrainiens dans de nombreux domaines tels que la cyberdéfense ou l'identification des mouvements de troupes ennemies. Mais aussi, en distillant des communiqués et des images avec une régularité de métronome, ils ont préparé le public occidental au conflit, et, ce faisant, ils ont probablement poussé le Kremlin à l'erreur.

Pour atteindre ce résultat, la CIA, la DIA, la NSA… se sont appuyées sur les sources traditionnelles (satellites militaires, écoutes électroniques, renseignement humain…) mais aussi sur une constellation de sources civiles ou PAI/CAI (*Publicly Available Information/Commercially Available Information*). En cela, le conflit ukrainien est bien une rupture non seulement dans la pratique de la guerre mais aussi celle du renseignement.

Pour l'illustrer, prenons Rechitsa, en Biélorussie, un camp militaire situé à 50 kilomètres de la frontière ukrainienne. Le 4 février 2022, une image satellite de la société Maxar, un opérateur commercial, révèle des rangées de véhicules militaires sous la neige. Quand le satellite repasse le 14 février, les véhicules ont disparu. Le lendemain, un blogueur repère l'un des régiments stationnés à Rechitsa sur une vidéo postée sur un réseau social, en route vers la frontière. L'information remonte à la CIA. Le schéma de l'invasion se dessine avec une clarté étonnante, privant les Russes de tout effet de surprise.

Prenons encore l'exemple de Yelnya, une base russe à l'ouest de la Russie. Mi-février, le 41e régiment interarmes, originaire de Sibérie, se volatilise entre deux passages d'un satellite commercial. À l'aide de la reconnaissance d'images, on retrouve un insigne du régiment « perdu » sur une vidéo téléchargée sur TikTok par un soldat russe. L'agrandissement du cliché permet d'identifier une gare, et même le numéro à huit chiffres d'un train, en provenance de… la base de Yelnya.

Depuis près de dix-huit mois, grâce à l'analyse systématique d'une quantité astronomique d'informations sources ouvertes, le renseignement américain étale les mouvements des troupes russes au grand jour, il annonce leurs opérations sous fausse bannière avant leur déclenchement, il fait l'état des pertes, prend le pouls du moral des soldats et de la population civile en entravant ainsi la propagande du Kremlin à chaque étape. Tout ceci n'aurait pas été possible sans l'OSINT.

La révolution de l'OSINT

Tout commence à l'aube des années 2010. L'Amérique n'en finit pas d'être en guerre contre le terrorisme. Malgré sa capacité de surveillance planétaire, le renseignement américain peine à identifier ses ennemis au cœur des vallées reculées de l'Afghanistan ou dans le désert irakien. Or, si les terroristes savent se cacher des satellites, ils ont tous un téléphone ; rapidement, l'analyse des réseaux sociaux couplée à celle des données de géolocalisation permet aux Américains de réaliser des assassinats ciblés à l'aide de drones pilotés à 10.000 kilomètres de distance. Pour la première fois, l'OSINT démontre sa valeur militaire face au renseignement électromagnétique (ROEM) et au renseignement humain (ROHUM).

Avec la croissance exponentielle des données numériques de type public ou commercial, cookies, adresses IP, « posts », pages web, fichiers wave, vidéos, images etc., la fameuse « poussière numérique », et celle des outils destinés à les analyser et les distribuer au reste du monde, l'OSINT s'invite dans les arcanes des services secrets américains, et cela a un coût « minime » si on le compare aux disciplines traditionnelles.

Rapidement, la communauté du renseignement mesure les innombrables possibilités offertes par cette corne d'abondance : des algorithmes fondés sur les mots-clés ou le langage naturel permettent d'identifier instantanément du contenu digne d'intérêt, de le catégoriser, de l'analyser, de le synthétiser; les logiciels de reconnaissance d'image facilitent l'examen de vidéos à grande échelle, des logiciels tels que SunCalc aident à déterminer l'heure précise d'un cliché en fonction de la longueur et du positionnement des ombres… La liste est infinie. Et les possibilités, illimitées.

Grâce à l'OSINT, il devient beaucoup plus facile de prévoir ou d'anticiper. C'est le recoupement des informations militaires, d'imagerie satellitaire commerciale, de réseaux sociaux et de données de géolocalisation qui ont permis de prédire l'invasion russe.

De plus, les sources ouvertes aident à « gérer » l'opinion, en livrant des informations confidentielles sur la place publique, sans risque de compromettre des sources classifiées, comme on l'a vu depuis le début de la crise ukrainienne. Armé d'une montagne de données, le renseignement peut les distiller au fur et à mesure, exerçant ainsi une pression constante sur ses adversaires, bien en peine de reprendre l'initiative dans la communication.

En traitant les données partagées sur les réseaux sociaux, l'OSINT peut analyser les mouvements de l'ennemi, faire l'état précis de ses échecs et ses succès, documenter les crimes de guerre…; avec les données de géolocalisation, il identifie les concentrations de soldats et permet de recouper les images obtenues des satellites militaires.

En résumé, grâce à la fusion des données ROSO et des sources ROEM et ROHUM, les analystes peuvent affiner leurs hypothèses, les enrichir, les comparer, les confirmer, tout cela à un coût marginal. Un rapport récent du RUSI [Royal United Services Institute for Defence and Security Studies, ndlr] estime le coût de l'OSINT à 1 % des budgets totaux contre 35 à 90 % des informations générées. La DIA évalue, quant à elle, à 80 % la part des informations d'origine sources ouvertes.

La transformation ne fait que commencer

C'est une révolution culturelle. D'abord, il faut recruter et intégrer des nouveaux métiers: des *data scientists* capables de traiter des volumes gigantesques de données brutes, des linguistes, des psychologues comportementaux, des programmeurs aptes à développer des algorithmes propriétaires, des professionnels des métiers de l'information à l'aise avec les derniers outils, et évidemment des analystes multidisciplinaires chargés de donner du sens à une matière brute, infinie.

Ensuite, les agences américaines de renseignement doivent construire des partenariats avec des acteurs commerciaux, grandes entreprises habituées à travailler avec l'État ou start-ups assises sur des montagnes de données numériques, et cela sans compromettre la nature confidentielle de leurs activités.

Et puis, elles doivent standardiser les protocoles, les procédures, de façon à normaliser l'analyse de bases de données non structurées, condition sine qua non d'une meilleure intégration des informations d'origine sources ouvertes avec les sources traditionnelles.

Enfin, se posent des difficultés d'ordre organisationnel. Comment décloisonner les départements et faciliter l'osmose des couches informationnelles ? Doit-on former les analystes classiques à l'exploitation de l'OSINT ou au contraire séparer les métiers ? Comment amalgamer les sources secrètes et publiques sans compromettre les unes et les autres ? Quels outils mettre en place pour identifier les tentatives de l'ennemi d'«empoisonner» les données ? Comment recruter, investir en intelligence artificielle, en big data, en supercalculateurs, en fermes de serveurs et en protocoles sécurisés suffisamment vite pour gérer le déluge exponentiel de *data* ?

La révolution est en marche. Le « nouveau » renseignement américain offre un modèle en construction aux agences étrangères désireuses de l'émuler. Nul doute que les romanciers d'espionnage sauront s'en inspirer pour inventer de nouveaux héros. Une chose est sûre: Bourne, Smiley ou Jack Ryan vont prendre un coup de vieux.