

# bellingcat

BELLINGCAT : JOURNALISTES OU AGENTS DE RENSEIGNEMENT ?

Par Adrien & Alexandre THUAU

LES PUBLICATIONS



## À PROPOS DE L'ARTICLE

Collectif indépendant de journalistes et de contributeurs locaux, Bellingcat s'est imposé comme un acteur de premier plan des relations internationales. Une utilisation méthodique et implacable des procédés de renseignement en sources ouvertes a permis au collectif de mettre au jour des crimes de guerre commis par le régime syrien, ou encore l'implication des forces armées russes dans le crash d'un avion dans le ciel du Donbass, en Ukraine. Sa notoriété s'est accrue grâce aux enquêtes successives menées au sujet des tentatives – avortées ou réussies – d'exécutions extrajudiciaires, perpétrées par les services de renseignement de la Fédération de Russie.

Cet article entend offrir au lecteur une description de la genèse et du développement de Bellingcat. La nature du collectif doit également être interrogée, à l'aune des méthodes employées pour les enquêtes sur la Russie. Le recueil de données en sources ouvertes, seule source des investigations du collectif, s'est doublée d'une infiltration de l'appareil d'État, posant la question de la mue du collectif – délibérée ou occasionnelle – en un organe de renseignement.

## À PROPOS DES AUTEURS

**Adrien THUAU** est membre du comité cyber des Jeunes de l'IHEDN et relecteur pour le pôle publication de l'association. Il finit ses études d'ingénieur en sécurité informatique.

**Alexandre THAU** est élève avocat, intéressé par les relations internationales et la géopolitique.

*Ce texte n'engage que la responsabilité des auteurs. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle.*

## Introduction

La littérature antique peut éclairer le rôle d'un nouvel acteur dans le jeu diplomatique contemporain. Dans une fable attribuée à Ésope, une communauté de souris tient conseil. Un chat, prédateur, menace la survie du groupe. Pour parer les attaques, une idée germe : lui faire porter un grelot permettrait de prévenir son arrivée, et de l'empêcher de nuire. Mais quand vient le moment d'élire celle d'entre elles chargée de passer le grelot autour du cou du chat, toutes se désistent, effrayées par le péril encouru. Deux leçons sont communément retirées de cette fable. La première consiste dans l'inutilité d'escompter un résultat, une finalité, si les moyens d'y parvenir sont illusoires ou voués à l'échec. La seconde met en exergue le courage d'une ou plusieurs personnes qui, en dépit du danger et conscientes de celui-ci, accomplissent des actions pour le bien commun.

La référence à la fable est revendiquée par Bellingcat, dont le nom même constitue la contraction de l'expression anglaise « belling the cat », par référence à la morale attribuée au texte. Or, le rôle d'aiguillon de Bellingcat, tant à l'égard du journalisme que des enjeux géopolitiques, est aujourd'hui tangible. Depuis plusieurs années, le collectif emmené par Elliot Higgins participe au décryptage de la diplomatie et de l'action militaire et clandestine dans un contexte de résurgence des États puissances, la Russie en tête.

Le sillon tracé par Bellingcat fait aujourd'hui des émules, au point qu'il est possible d'interroger la démarche du collectif. Par ses méthodes, Bellingcat a-t-il introduit une révolution dans la manière d'étudier et de décrypter la politique étrangère des États ? Plus encore, Bellingcat est-il le résultat d'un syncrétisme, mêlant codes journalistiques traditionnels et méthodes empruntées au domaine du renseignement ?

Cette dernière question se pose avec une acuité nouvelle depuis la publication par le collectif d'enquêtes, largement relayées, sur les services de renseignement russes et leurs actions clandestines – crash du vol 17 abattu au-dessus du Donbass, affaires Skripal et Kangoshvili. Ces dernières semaines, le collectif s'est associé à l'activiste politique russe Alexeï Navalny, principal opposant politique du Kremlin, afin de dévoiler les efforts déployés par le FSB, service de renseignement intérieur de la Russie, pour traquer et empoisonner l'opposant. Non contents de mettre au jour les capacités technologiques du service et l'identité des agents impliqués, Bellingcat et Alexeï Navalny ont obtenu les confidences circonstanciées de l'un d'entre eux, en lui faisant croire qu'il parlait à un officier supérieur mandaté par le Kremlin pour faire la lumière sur les raisons de la faillite de l'opération.

L'immixtion de Bellingcat dans les rapports de force diplomatiques, à dessein ou involontairement, est désormais patente. L'organisation peut, à ce titre, être considérée alternativement comme un partenaire ou un adversaire par les États en présence. Cet état de fait interroge sur le rôle tenu par Bellingcat : s'agit-il d'un collectif indépendant, ainsi qu'il se revendique ? Ou poursuit-il sciemment des

intérêts convergents avec certains États, singulièrement ceux composant le bloc antagoniste à la Russie ? Cette question, à laquelle il serait présomptueux de trouver une réponse claire, mérite d'être posée, à l'aune des derniers développements de Bellingcat et des collaborations établies entre certaines institutions et le collectif.

Cet article se propose donc de présenter Bellingcat, les conditions de sa création et ses objectifs revendiqués. Cette première partie constitue un préalable à l'étude de l'utilisation par les journalistes des méthodes de renseignement en sources ouvertes. Le recours à ce mode d'investigation interroge sur la place occupée par Bellingcat dans les paysages institutionnel et géopolitique actuels.

## Bellingcat : entre journalisme et activisme international

Bellingcat est un collectif de chercheurs, de journalistes et de citoyens qui, selon la description faite sur le site éponyme, mettent en commun des compétences et des méthodes afin d'enquêter sur des sujets relatifs, dans leur grande majorité, à la politique étrangère des États.

Ce collectif est fondé en 2014 par Elliot Higgins, citoyen anglais résidant à Leicester, dont le parcours est relaté par *The Guardian*, dans un article publié en juin 2020<sup>1</sup>. Selon les éléments biographiques connus, l'intérêt d'Higgins pour les sujets géopolitiques n'est pas récent. Avant de mettre en œuvre les méthodes qui font aujourd'hui sa renommée, il s'intéresse depuis plusieurs années déjà à la politique étrangère des États-Unis, en Irak notamment. Cet intérêt se concrétise en 2012, alors que la Syrie sombre dans la guerre. Sous le pseudonyme Brown Moses, Higgins commente des articles de blogs hébergés par *The Guardian*. D'abord épisodiques, ses recherches s'étoffent, jusqu'à l'ouverture de son propre blog, sur lequel il publie le fruit de ses enquêtes.

Son audience, d'abord confidentielle, s'élargit en quelques mois. Le travail d'Higgins est salué par le double prix Pulitzer Christopher John Chivers qui, dans le *New York Times* en 2013, cite son enquête sur l'approvisionnement en armes croates des groupes djihadistes par l'Arabie Saoudite<sup>2</sup>. L'enquêteur amateur persiste : parmi ses premières révélations figure la démonstration de la détention d'armes à fragmentation par le régime syrien. S'agrègent progressivement autour de lui, au gré de ses publications, enquêteurs et journalistes, amateurs ou professionnels.

C'est dans ce contexte qu'est créé Bellingcat. Le collectif se veut collaboratif, et fondé sur la mise en commun de compétences techniques, propices à la mise en œuvre de techniques d'investigation fondées sur les méthodes du renseignement en sources ouvertes<sup>3</sup>. Toutes les enquêtes menées sur Bellingcat se fondent sur une méthode commune : l'utilisation des réseaux sociaux (Twitter), des

---

<sup>1</sup> *The Guardian*, 23 juin 2020, "A chain of stupidity" : the Skripal case and the decline of Russia's spy agencies.

<sup>2</sup> *The New York Times*, 25 février 2013, C.J. Chivers et E. Schmitt, Saudis Step Up Help For Rebels in Syria With Croatian Arms.

<sup>3</sup> Nous reviendrons sur ce concept dans la suite de l'article.

plateformes de vidéo (YouTube) et des sites de visualisation de photographies aériennes et satellitaires (Google Earth). À partir de contenus audiovisuels le plus souvent, Bellingcat enquête afin de donner une date, un lieu, des mobiles et des identités à des faits et des individus.

Bellingcat a couvert, depuis près de six ans, un large éventail de sujets. La démonstration de l'utilisation d'armes chimiques par le régime de Bachar Al-Assad, dans la région de Ghouta près de Damas, constitue l'un de ses premiers faits d'armes. La localisation du lieu d'exécution de James Foley, journaliste américain otage de l'État islamique donne un écho nouveau aux méthodes employées par le collectif, fondées en l'espèce sur l'exploitation d'images satellites publiques, l'analyse de la végétation environnante et des ombres projetées par le soleil.

Une enquête, au retentissement notable, offre un condensé riche d'enseignements sur les procédés d'investigation dont use le collectif. Un documentaire d'une dizaine de minutes, fruit d'un travail conjoint mené par Amnesty International, Bellingcat et Africa Eye, le service d'investigation de BBC Africa, met au jour les méthodes employées pour localiser et dater la commission d'une bavure criminelle par l'armée régulière camerounaise, dans le Nord du pays. La vidéo montre l'exécution sommaire de femmes et d'enfants accusés d'accointances avec Boko Haram, mouvement islamiste terroriste et insurrectionnel. L'enquête, largement relayée, a provoqué l'arrestation des militaires identifiés dans la vidéo, et leur condamnation en 2020 par la justice camerounaise.

Plus récemment, l'audience de Bellingcat s'est encore élargie à l'aune des études publiées par le collectif sur la Russie. Plusieurs affaires ont mis en lumière les assassinats extrajudiciaires avortés et réussis du renseignement militaire russe, le GRU. L'affaire dite Skripal, du nom d'un ancien officier du renseignement militaire russe recruté par les services du Royaume-Uni, arrêté et condamné en Russie, puis échangé contre des agents russes sous couverture, démasqués par les services occidentaux, en constitue l'exemple le plus médiatique. L'enquête minutieuse menée sur l'assassinat à Berlin d'un ancien insurgé géorgien de la guerre qui a opposé l'État du Caucase à la Russie, a retracé le parcours suivi par l'auteur présumé de l'exécution. Mis en cause quelques années auparavant dans l'assassinat d'un homme d'affaires à Moscou, le suspect avait bénéficié de l'annulation du mandat d'arrêt le visant en 2015. Depuis l'assassinat commis dans la capitale allemande, Bellingcat a révélé que le suspect a bénéficié du concours d'un service fédéral russe pour obtenir son passeport, institution déjà à l'origine de l'émission des passeports des agents impliqués dans l'affaire Skripal. De similaires perméabilités bureaucratiques ont ouvert la voie à la démonstration de la collaboration effective entre le renseignement militaire russe et la société paramilitaire Wagner, dont les contractuels sont impliqués dans les théâtres d'opération de la Russie au Moyen-Orient. Ces démonstrations, plus largement documentées aujourd'hui à l'aune des enquêtes menées par la presse, ont d'abord été le fait du collectif.

Ces publications sont typiques des méthodes employées par cet organisme. Bellingcat a fait du renseignement en sources ouvertes le principe de ses investigations. Ce type de source est désigné par les acronymes ROSO (renseignement d'origine source ouverte) dans le renseignement français et OSINT (Open Source INTelligence) dans une dénomination plus universelle venue des États-Unis. Les définitions du renseignement en source ouverte sont multiples ; les principales divergences s'articulent autour du champ de définition des sources dites « ouvertes ». Il est toutefois possible de définir la source ouverte comme une source dont l'accès est public. Sans aucun doute, les sites Internet Google Earth ou YouTube constituent des sources ouvertes. Il en est de même pour le réseau social Twitter. L'existence d'une barrière tarifaire (l'abonnement à une base de données par exemple) pose déjà la question de l'appartenance de la source à la sphère publique. De manière générale, le renseignement en source ouverte provient essentiellement des plateformes numériques. À l'inverse, le recours à du renseignement de source humaine (HUMINT) ne constitue pas, à proprement parler, une source ouverte, dès lors qu'il implique de pouvoir avoir accès à la personne dépositaire de la donnée ou de l'information recherchée.

Ainsi, si le collectif n'a bien sûr pas la primeur du recours à l'investigation en sources ouvertes, son institutionnalisation a sans doute constitué une évolution profonde dans la manière de produire de l'information.

Plus récemment, Bellingcat a pu recourir à des sources ne relevant plus de la catégorie des sources ouvertes. Cette évolution, brièvement évoquée à propos des assassinats extrajudiciaires accomplis par la Russie, marque peut-être un changement de paradigme, qu'il conviendra d'évoquer ensuite.

## L'exploitation du renseignement en source ouverte

Le travail journalistique fourni par Bellingcat doit être interprété à l'aune des méthodes utilisées. En effet, le collectif s'est d'abord différencié par les procédés employés. À sa création, les articles publiés utilisaient exclusivement des sources ouvertes. Afin de mieux comprendre le processus d'investigation utilisé, revenons sur une enquête qui met en exergue les compétences déployées.

En août 2017, la Cour pénale internationale émet un mandat d'arrêt international contre Mahmoud Mustafa Busayf Al-Werfalli, commandant de la brigade Al-Saiqa au sein de l'armée nationale libyenne. Il est en effet accusé d'avoir supervisé des exécutions de masse. Singularité remarquable : ce mandat d'arrêt se fonde uniquement sur la base d'éléments de preuves recueillis en sources ouvertes, des réseaux sociaux en majorité. Le 3 octobre 2017, Bellingcat publie un article<sup>4</sup> expliquant comment ses

---

<sup>4</sup> Bellingcat, « How a Werfalli Execution Site Was Geolocated », 3 octobre 2017, <https://www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated> [Dernière consultation : 25/01/2021].

équipes d'investigation ont localisé un des sites d'exécution mentionnés par la Cour pénale internationale.

À l'origine de l'enquête, une vidéo Facebook publiée fin juillet 2017 met en scène l'exécution de 20 otages décrits comme membres de l'État islamique. Sur cette base, Bellingcat commence son travail d'investigation. Le but : localiser l'endroit exact de l'exécution. Le processus s'annonce complexe ; les images montrent un endroit désertique, qui n'offre que de maigres points d'appui afin d'établir le lieu de commission des faits. Les seuls éléments distinctifs sont un morceau de bâtiment qui apparaît moins d'une seconde, quelques buissons visibles à l'arrière-plan et deux pistes marquées par des véhicules dans le sable. Les experts de Bellingcat se mettent à l'œuvre.

Le sable leur permet de réduire la zone de recherche : sa couleur grisâtre leur indique qu'il s'agit probablement d'un lieu au sud-ouest de Benghazi où le sable est moins jaune qu'ailleurs. L'architecture du bâtiment est ensuite analysée. Il ne semble pas terminé. À partir des images de Google Earth et du site WikiMapia, Bellingcat remonte jusqu'à un projet immobilier chinois qui n'a jamais vu le jour à cause de la guerre civile libyenne. Cependant, l'étendue du complexe ne permet pas d'établir le lieu exact : tous les bâtiments se ressemblent sur plusieurs centaines de mètres.

Bellingcat analyse alors plusieurs autres vidéos du compte Facebook à l'origine de la publication initiale. Tournées dans la même zone, elles permettent aux journalistes de repérer une clôture. En suivant son tracé sur Google Earth, ils repèrent des chemins dans le sable. Grâce à des comparaisons de la végétation environnante, le lieu de l'exécution est précisément identifié ; aucun doute n'est possible, les éléments du paysage correspondent parfaitement. Quelques recherches sur le site d'imagerie TerraServer permettent d'apporter un élément supplémentaire : quelques jours après la date potentielle de l'exécution, des traces apparaissent au sol sur le lieu présumé. Elles correspondent aux tâches de sang laissées lors de l'exécution des prisonniers. Grâce à ces éléments supplémentaires, Bellingcat estime approximativement l'heure de la vidéo. Les ombres apparues dans l'enregistrement permettent d'établir l'heure exacte. Pour ce faire, le collectif a utilisé le site SunCalc. Il permet de mesurer les ombres en fonction de la position du soleil dans la journée.

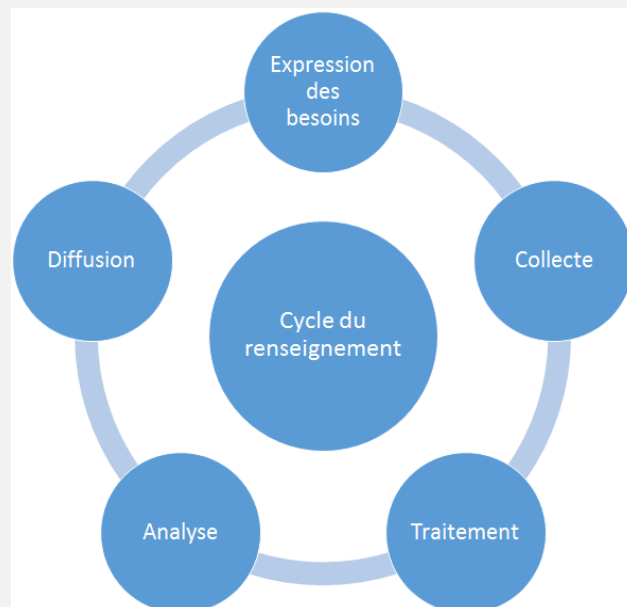
Le niveau technique mis en œuvre pour arriver à ces résultats est remarquable. Bien que l'OSINT soit utilisé dans le cadre du journalisme d'investigation, les détails techniques du processus de recherche sont rarement décrits de façon aussi transparente que dans les articles de Bellingcat. Ces méthodes permettent au collectif britannique de s'affranchir des problématiques de protection des sources : elles sont ouvertes à tous, ce qui fait l'essence des articles de Bellingcat – au moins pour leurs premières enquêtes.

Ce point n'est pas marginal. Il change la nature même du journalisme d'investigation, dans lequel la transparence des enquêtes se heurte souvent à la protection des sources, afin d'assurer leur sécurité

ou la pérennité de leur situation privilégiée, qui est exploitée par les journalistes. Lire un article de Bellingcat implique de pouvoir retracer soi-même le déroulé de l'enquête. Le lecteur peut vérifier sans difficulté les lieux décrits sur Google Earth, ou les données utilisées lors des enquêtes.

Il est important de noter que Bellingcat ne se contente pas de relayer de l'information ouverte. La valeur des articles réside dans le travail d'analyse qui est fourni : comparaison, recoupements, contextualisation, etc.

Profitons-en pour différencier Bellingcat d'une ONG désormais célèbre pour ses révélations : Wikileaks. Les publications de Wikileaks contiennent principalement des données ou de l'information. Ces dernières ne sont pas nécessairement contextualisées ou recoupées : elles demandent un travail journalistique conséquent avant de pouvoir être publiées sous forme d'article. Cela permet à l'ONG de publier le fruit de ses recherches plus rapidement, notamment afin de s'affranchir de pressions extérieures. Les enquêtes de Bellingcat, au contraire, nécessitent un travail sur un temps parfois long (plusieurs semaines, voire plusieurs mois) avant d'aboutir à un article. Bellingcat fournit des connaissances, voire du renseignement, là où Wikileaks fournit principalement de l'information brute. À cet égard, il est intéressant de comparer le processus journalistique de l'association avec la production de renseignement. Pour ce faire, revenons sur le « cycle du renseignement ». Cette figure permet de synthétiser les étapes de production du renseignement. Elle permet aussi de comprendre en quoi les recherches de Bellingcat peuvent être comparés à ceux d'un service de renseignement, et ce par ses méthodes, non par ses finalités.



LE CYCLE DU RENSEIGNEMENT<sup>5</sup>

<sup>5</sup> [https://fr.wikipedia.org/wiki/Fichier:Cycle\\_du\\_renseignement.png](https://fr.wikipedia.org/wiki/Fichier:Cycle_du_renseignement.png).



La première étape dans la production de renseignement est l'expression du besoin. Chez Bellingcat, le besoin est identifié en interne, par les équipes de l'association. Dans un service de renseignement, cette expression a pour origine des consignes hiérarchiques, ou une opportunité d'acquérir des informations.

Vient ensuite la collecte des données. Pour Bellingcat, c'est à cette étape que le renseignement en source ouverte trouve sa pleine mesure : toutes les sources consultées sont publiques. Bien qu'un service de renseignement utilise aussi des sources publiques, les moyens de collecte sont plus variés, et comprennent aussi des sources dites fermées.

Les données brutes récoltées sont ensuite traitées : cette étape leur permet de devenir des informations. Il s'agit alors de replacer la donnée collectée dans un contexte, de la traduire afin de la rendre intelligible. Parfois, la collecte inclut aussi directement des informations. Ces dernières sont ensuite comparées, contextualisées, grâce à des connaissances humaines afin d'en retirer un renseignement. Dans le cas de Bellingcat, ces renseignements sont mis en forme pour publier un article. Pour un service de renseignement, ils permettent de diffuser une note à destination des commanditaires, souvent sous le joug du secret de la défense nationale.

Le travail de l'organe de presse britannique est donc comparable à celui d'un service de renseignement. Deux points majeurs diffèrent : les sources exclusivement ouvertes et la diffusion de la production. Bellingcat a fait de ces caractéristiques une force : la connaissance produite est diffusée très largement, sans être réservée à un sous-ensemble qui en retire une puissance stratégique. La transparence du collectif, érigée en principe journalistique, permet aux lecteurs de s'approprier le contenu publié, voire, à terme, de participer aux enquêtes. De plus, les renseignements produits par le collectif peuvent être soumis à un processus de vérification communautaire, ce qui permet d'affiner des publications éventuellement incomplètes.

En somme, Bellingcat s'inscrit dans le journalisme d'investigation tout en bouleversant ses méthodes. Parfois citée comme texte fondateur de la déontologie du journalisme, la Charte de Munich liste les droits et devoirs du journaliste<sup>6</sup>. Nous reproduisons ici ces obligations:

1. Respecter la vérité, quelles qu'en puissent être les conséquences pour lui-même, et ce, en raison du droit que le public a de connaître la vérité.
2. Défendre la liberté de l'information, du commentaire et de la critique.
3. Publier seulement les informations dont l'origine est connue ou les accompagner, si c'est nécessaire, des réserves qui s'imposent ; ne pas supprimer les informations essentielles et ne pas altérer les textes et les documents.

---

<sup>6</sup> [https://fr.wikipedia.org/wiki/Charte\\_de\\_Munich](https://fr.wikipedia.org/wiki/Charte_de_Munich) [Dernière consultation : 25/01/2021].

4. Ne pas user de méthodes déloyales pour obtenir des informations, des photographies et des documents.
5. S'obliger à respecter la vie privée des personnes.
6. Rectifier toute information publiée qui se révèle inexacte.
7. Garder le secret professionnel et ne pas divulguer la source des informations obtenues confidentiellement.
8. S'interdire le plagiat, la calomnie, la diffamation, les accusations sans fondement ainsi que de recevoir un quelconque avantage en raison de la publication ou de la suppression d'une information.
9. Ne jamais confondre le métier de journaliste avec celui du publicitaire ou du propagandiste ; n'accepter aucune consigne, directe ou indirecte, des annonceurs.
10. Refuser toute pression et n'accepter de directives rédactionnelles que des responsables de la rédaction.

Sans s'affranchir de ces responsabilités, le collectif, par ses méthodes d'enquête et d'analyse, peut se permettre de dévoiler ses sources. En effet : elles sont publiques. Ainsi, l'authenticité et la probité des informations peuvent être facilement vérifiées par les lecteurs.

À l'instar d'autres médias, la ligne éditoriale de Bellingcat repose principalement sur l'investigation. Cependant, le caractère collaboratif et non professionnel d'une partie de ses équipes le distingue d'une rédaction classique. La professionnalisation du collectif est toutefois croissante, à mesure que des journalistes collaborent activement à la rédaction des articles et à leur traduction.

La qualité technique mise en œuvre et la transparence des processus qui concourent à la rédaction des articles donnent corps à l'objectif poursuivi par le collectif : donner du pouvoir aux citoyens en publiant de l'information analysée, tout en présentant les outils qui permettent de le faire. C'est pourquoi Bellingcat doit être différencié du journalisme d'investigation traditionnel, grâce auquel le lecteur se voit présenter le résultat des investigations, mais rarement la méthode ayant permis d'y aboutir. Le lecteur de Bellingcat peut d'ailleurs prendre une part active à la vie de Bellingcat ; des formations sont organisées, afin d'intégrer de nouveaux talents. Il s'agit de la principale méthode de croissance de Bellingcat.

La charte de Munich est tout aussi utile pour mettre en perspective l'évolution de Bellingcat depuis sa création. L'utilisation dans plusieurs enquêtes de sources non publiques, voire humaines, remet en cause toutes les caractéristiques discutées jusqu'alors. L'OSINT n'a plus l'exclusivité dans les enquêtes publiées. Par conséquent, la transparence des articles n'est plus totale.

Ce changement de paradigme est patent dans la succession d'articles de Bellingcat relatifs aux actions clandestines russes. Conséquemment, le statut de l'organisation a évolué, jusqu'à influencer les

relations internationales. Cette immixtion dans les sphères de la diplomatie et de la défense, volontaire ou non, pose la question de la neutralité politique du travail conduit par Bellingcat. Cette question, qui ne saurait supporter une réponse définitive, permet d'établir des hypothèses.

## Un acteur paraétatique du renseignement ?

Les enquêtes récentes menées par Bellingcat au sujet de la Russie suscitent des interrogations quant aux objectifs poursuivis par le collectif. Le retentissement rencontré par ces publications, du fait du pays qu'elle visait, ont projeté encore davantage Bellingcat sur le devant de la scène. L'affaire dite Skripal, ainsi que l'assassinat perpétré à Berlin décrit plus haut, ont jeté une lumière crue sur les méthodes et les errements du service de renseignement militaire russe, le GRU. Les investigations menées par Bellingcat sur ces deux crimes s'appuient pour partie sur la consultation de bases de données de services administratifs ou de police russes, auxquelles Bellingcat a obtenu l'accès par l'intermédiaire de sources internes<sup>7</sup>. Relatées par les articles écrits au sujet de l'assassinat commis à Berlin contre le milicien géorgien, dans lequel l'implication du FSB – service de renseignement fédéral russe, dont la compétence s'étend, en théorie, au territoire de la Fédération de Russie – est étayée, les informations obtenues par l'intermédiaire de bases de données ont également permis à Bellingcat d'étudier les déplacements des agents identifiés comme auteurs de l'empoisonnement de Sergueï et Julia Skripal<sup>8</sup>. En l'espèce, des métadonnées permettant de géolocaliser l'un des agents ont été obtenues grâce à une source travaillant au sein de l'opérateur téléphonique auprès de qui la ligne était enregistrée.

Outre l'influence que ces révélations ont eu pour la Russie, tant sur le plan diplomatique qu'à l'égard de sa capacité à mener des actions clandestines hors de ses frontières, les publications de Bellingcat s'appuient sur des méthodes différentes de celles qui avaient accompagné sa création et son activité jusqu'alors.

La récurrence des enquêtes réalisées au sujet de la Russie soulève elle aussi plusieurs questions. La première porte sur la raison de ce prisme russe. Faut-il y voir une opportunité saisie par Bellingcat, ou l'expression d'une volonté nouvelle à l'aune des derniers développements géopolitiques, auxquels la Russie prend une large part ?

Une série de raisons incitent à voir dans cette tendance l'expression d'un opportunisme. La première a trait aux informations dont Bellingcat dispose pour servir ses enquêtes.

---

<sup>7</sup> Bellingcat, « Identifying The Berlin Bicycle Assassin: Russia's Murder Franchise (Part 2) », 6 décembre 2019.

<sup>8</sup> Bellingcat, « The GRU Globetrotters: Mission London », 28 juin 2019.

De nombreux outils utilisés par les citoyens russes sont particulièrement utiles s'agissant du renseignement en sources ouvertes.

Vkontakte, réseau social russe, constitue une mine de données précieuses. Utilisé majoritairement par la communauté russophone, repris en main en 2014 par le Kremlin après l'éviction de son fondateur Pavel Dourov, le site se veut le pendant russe de Facebook. Il est, à ce titre, et de manière étonnante, utilisé par des membres des services de renseignement et des unités d'élite de l'armée russe. Vkontakte a ainsi pu permettre à Bellingcat d'effectuer des recoupements afin, par exemple, d'étayer la présence de Spetsnaz dans l'Est ukrainien à partir des années 2014. Ces vérifications ont été rendues possibles par l'expertise de Bellingcat en matière de localisation précise de photographies, mais aussi par certaines caractéristiques techniques de la plateforme. En effet, les principaux réseaux sociaux occidentaux prennent des mesures pour protéger les métadonnées publiées par leurs utilisateurs. De telles mesures ne sont pas appliquées de manière drastique par Vkontakte qui se montre moins regardant. Les métadonnées des photos postées par les utilisateurs ne sont par exemple pas nettoyées par la plateforme avant leur publication, contrairement à Facebook ou Instagram. Ainsi, de nombreuses photos postées depuis un smartphone renseignent par exemple la localisation exacte au moment de la photo, voire le modèle de l'appareil. Ces informations se sont souvent avérées extrêmement précieuses pour Bellingcat.

D'autres outils spécifiques à l'écosystème russe ont permis à Bellingcat de recouper des données lors d'enquêtes majeures. Yandex, moteur de recherche particulièrement efficace pour la recherche inversée d'images (recherche de pages web à partir d'une image) est à cet égard un exemple édifiant. Par ailleurs, le collectif britannique recourt de manière récurrente à FindFace, outil de reconnaissance faciale qui leur a permis de retrouver des profils Vkontakte à partir de photos d'individus jusqu'alors non identifiés<sup>9</sup>.

En effet, là s'incarne sans doute la pièce maîtresse des enquêtes du collectif sur la Russie. Bellingcat consulte depuis plusieurs mois des bases de données administratives, recensant les passeports délivrés à des ressortissants russes. Figurent également les adresses renseignées par les demandeurs. C'est par ce truchement que Bellingcat a pu, notamment, confronter l'identité de couverture des agents du GRU dépêchés à Salisbury pour empoisonner Sergueï Skripal, à leur véritable identité. Erreur grossière des services : les deux agents étaient réputés habiter dans un immeuble constituant une dépendance et abritant des logements de fonction dévolus aux personnels du renseignement militaire.

---

<sup>9</sup> Le succès de l'application a d'ailleurs été tel qu'elle n'est désormais plus disponible gratuitement. La puissance de ce logiciel s'échange désormais contre d'importants contrats signés avec l'entreprise.

La disponibilité d'informations à haute valeur ajoutée ainsi que les négligences coupables des services de renseignement russes ont permis au collectif de mener des enquêtes fournies au retentissement international. Cependant, toutes les publications répondaient à la même méthode, ciblant le même sujet : les erreurs répétées du GRU – que des observateurs avisés ont qualifié d'amateurisme –, impliqué dans plusieurs scandales internationaux. Le FSB n'est pas en reste : comme évoqué plus haut, l'analyse des métadonnées du téléphone portable du suspect a permis d'établir sa présence sur un site d'entraînement des personnels du FSB, ainsi que ses contacts avec des membres actifs et retraités du département « V », bras armé du service de renseignement. L'utilisation des bases de données russes, qui recensent les détenteurs de passeports russes, a permis d'effectuer des recoupements et de confirmer l'identité véritable du suspect.

Plus récemment, l'affaire Navalny a permis au collectif de décrire de façon encore plus précise ses méthodes : une publication dédiée<sup>10</sup> aux aspects techniques a accompagné l'article principal. Elle avait pour but de décrire les techniques employées, notamment l'accès rapide à des informations sensibles en échange de l'équivalent de quelques dizaines d'euros<sup>11</sup>.

Ces éléments propices aux investigations n'expliquent pas, à eux seuls, les résultats impressionnants engrangés par Bellingcat. Les articles publiés ne dissimulent rien des complicités internes à l'administration russe ayant permis l'accès aux bases de données. Dès lors, le renseignement en source ouverte se double d'un renseignement non ouvert, d'origine humaine. Cette évolution significative interroge, à plusieurs égards.

Elle pose la question de la gestion par Bellingcat de la dimension humaine du renseignement qu'il produit. Le collectif doit désormais protéger ses sources, de manière à pouvoir les solliciter, et surtout de sorte qu'elles ne soient pas exposées à des risques qui, loin d'être hypothétiques, sont tout à fait plausibles eu égard à l'atteinte qu'elles portent au secret des intérêts russes. Le préjudice causé à la Russie par ces révélations est extraordinaire. Certes, la communauté internationale, le Royaume-Uni en tête, n'a pas attendu les révélations de Bellingcat pour prendre des mesures de rétorsion – la plus importante étant l'expulsion de dizaines de diplomates russes –, déstabilisant de fait le réseau de renseignement tissé par le Kremlin dans les pays occidentaux. Mais les enquêtes publiées ont rendu publics des faits et des corrélations qui étaient jusqu'alors l'apanage des services de renseignement et de contre-espionnage. La violence de la campagne de communication menée par l'État russe, par l'intermédiaire d'une conférence de presse du ministère de la Défense russe notamment, témoigne de l'importance du préjudice causé.

<sup>10</sup> <https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology> [Dernière consultation : 25/01/2021].

<sup>11</sup> Le collectif a notamment eu recours à plusieurs bots Telegram leur permettant d'obtenir des informations précises (adresse, véhicule, etc.) de citoyens russes travaillant pour les renseignements extérieurs.

En tout état de cause, le changement de méthode de Bellingcat, apprécié à l'aune de son rôle dans les relations internationales et le cours de la géopolitique pose la question de sa définition. Alors que le renseignement en sources ouvertes, collecté et exploité par des contributeurs d'horizons divers, constituait sa raison d'être en même temps que son principe, il semble que ces éléments ne suffisent plus à décrire Bellingcat. Alors que le collectif se donnait pour objectif de réarmer le lecteur, avisé ou profane, afin de lui permettre de comprendre les processus d'enquête et les méthodes d'investigation, le recours à des sources fermées ne contrevient-il pas à cette visée ?

Plus encore, Bellingcat se présente traditionnellement comme un médium citoyen. Les enquêtes sur la Russie ont été rendues possible par une infiltration de l'appareil d'État, par des procédés que n'auraient pas reniés les services de renseignements étatiques. Ce faisant, Bellingcat ne devient-il pas un plein acteur des relations internationales et, à ce titre, un adversaire désigné de la Russie ?

Ces questions n'appellent pas de réponse formelle, dès lors que le collectif ne communique pas officiellement sur ces points. Quelques éléments peuvent toutefois alimenter le débat sur l'indépendance du collectif.

L'affranchissement de Bellingcat de toute tutelle étatique, ou politique, s'envisage aussi à l'aune de ses soutiens financiers et politiques. Une étude des soutiens de Bellingcat, depuis le site du collectif, révèle des liens parfois étroits avec des organisations liées aux gouvernements occidentaux. Outre le soutien et le financement par des trusts (Sigrid Rausing Trust), des fonds de dotation (Auxilium) ou des fondations philanthropiques (Porticus), Bellingcat bénéficie par exemple de l'appui de l'organisation non-gouvernementale National Endowment for Democracy (NED). Cette dernière se décrit comme indépendante, mais ne dissimule rien de son financement par le Congrès américain.

Il ne s'agit pas du seul lien entre Bellingcat et des gouvernements. En 2015, alors commandant suprême des forces de l'OTAN en Europe, le général Philip Breedlove fait, sur son compte Twitter, la promotion de l'enquête participative de Bellingcat au sujet de l'implication russe dans le conflit ouvert en cours dans l'Est ukrainien<sup>12</sup>. De la même façon, l'ambassade britannique en Ukraine a pu, en 2016, relayer un article au sujet du crash de l'avion MH17 dans le Donbass ukrainien, en présentant Elliot Higgins comme la némésis de Vladimir Poutine<sup>13</sup>. L'ambassadeur britannique en Grèce, par la voie de son compte Twitter institutionnel, s'est également fait l'écho de l'enquête de Bellingcat démontrant l'implication des forces armées russes au côté des séparatistes ukrainiens<sup>14</sup>.

L'indépendance de Bellingcat ne saurait être remise en cause du fait de ces quelques éléments. Ces financements et cette appropriation ne suffisent pas à remettre en cause la probité de la démarche de

<sup>12</sup> <https://twitter.com/PMBreedlove/status/564855335627018242?s=20> [Dernière consultation : 25/01/2021].

<sup>13</sup> <https://twitter.com/UKinUkraine/status/684016232136359936?s=20> [Dernière consultation : 25/01/2021].

<sup>14</sup> <https://twitter.com/USAmbPyatt/status/688994797990883329?s=20> [Dernière consultation : 25/01/2021].

Bellingcat. Cependant, ils peuvent jeter le discrédit, voire l'opprobre, alors que les relations avec la Russie se sont notoirement dégradées au cours de la décennie 2010.

De plus, le colossal travail de collecte d'informations par Bellingcat peut être valorisé par ces gouvernements qui, par de leur propre fait ou par l'intermédiaire d'associations – parmi lesquels Amnesty International<sup>15</sup> – souhaitent utiliser ces données afin de documenter des conflits, ainsi que les crimes de guerre ou crimes contre l'humanité qui auraient été commis durant leur déroulement<sup>16</sup>. Le conflit syrien est à cet égard un exemple édifiant, les enquêtes menées par les contributeurs ayant permis d'étayer l'implication de plusieurs militaires syriens dans une attaque chimique<sup>17</sup>.

## Conclusion

En somme, Bellingcat est un objet d'étude dont les contours sont flous. La présentation parcellaire de ses travaux donne à voir un collectif empruntant des méthodes au journalisme d'investigation autant qu'au renseignement. À cet égard, l'utilisation de données pourvues par un fonctionnaire de l'administration russe a fait entrer le collectif dans le domaine des sources fermées, voie utilisée par les journalistes, mais également matrice traditionnelle des services de renseignement étatiques. L'objectif poursuivi, justifiant de l'emploi de la méthode, incite à distinguer Bellingcat d'un simple collectif d'enquêteurs au service de l'information citoyenne. Pour autant, assimiler Bellingcat à un organe de renseignement privé serait fallacieux. Sans doute les prochaines orientations du collectif permettront d'étoffer l'analyse.

Il est toutefois indéniable que Bellingcat est aujourd'hui partie prenante des relations internationales. Les enquêtes rendent publics des éléments dont la connaissance n'appartenait jusqu'alors qu'à des organes de renseignements étatiques. Une telle implication n'est donc pas négligeable. La collaboration ou la promotion du collectif par des gouvernements et des associations, entretenant des liens étayés avec des États, témoigne de l'institutionnalisation du collectif. Sans remettre en cause l'indépendance de ses travaux, de telles relations témoignent du bénéfice retiré par des États intéressés par l'activisme russe sur la scène géopolitique.

---

<sup>15</sup> <https://www.amnesty.org/fr/latest/news/2018/04/how-open-source-evidence-took-a-lead-role-in-the-response-to-the-douma-chemical-weapons-attack/> [Dernière consultation : 25/01/2021].

<sup>16</sup> Amnesty International, « Les investigations d'Amnesty International à partir d'informations issues de sources libres d'accès », <https://www.amnesty.org/fr/latest/news/2018/09/digitally-dissecting-atrocities-amnesty-internationals-open-source-investigations/> [Dernière consultation : 25/01/2021].

<sup>17</sup> Korii, Antoine Hasday, « Quand les outils numériques dévoilent des crimes de guerre », <https://korii.slate.fr/et-caetera/syrie-bellingcat-enquete-open-source-crimes-guerre-regime-bachar-el-assad-attaque-chimique-latamne> [Dernière consultation : 25/01/2021].



[publications@jeunes-ihedn.org](mailto:publications@jeunes-ihedn.org)