Politique de sécurité: **analyses du CSS**

CSS ETH Zurich

N° 32 • avril 2008 • 3ème année

OPEN SOURCE INTELLIGENCE: NOUVEAU PARADIGME DU RENSEIGNEMENT?

L'importance du renseignement en sources ouvertes a augmenté ces dernières années. Pour les services de renseignement, l'*Open Source Intelligence* restera simplement une manière de recueillir des renseignements parmi d'autres. Mais, pour beaucoup d'autres services gouvernementaux, l'OSINT est souvent le seul moyen d'obtenir des informations. L'élaboration d'une stratégie OSINT nationale et la mise sur pied d'un centre OSINT sont des mesures dignes d'être examinées de manière à pouvoir exploiter plus systématiquement les informations provenant de sources ouvertes.

www.istockphoto.com

Le concept d'*Open Source Intelligence* a pris de l'importance ces dernières années. Autrefois, les services de renseignement s'occupaient surtout de recueillir et d'évaluer des informations classifiées. Les sources prépondérantes d'information comprenaient le renseignement humain (*human intelligence*, HUMINT), le renseignement électronique (*signals intelligence*, SIGINT) ainsi que le renseignement image (*imagery intelligence*, IMINT). Bien que des sources ouvertes aient aussi été souvent utilisées, elles ne représentaient qu'un outil complémentaire. Collecter systématiquement des informations non secrètes ne constituait pas une priorité des services secrets, ce qui était dû entre autres à la nature surtout militaire des domaines nécessitant ces informations.

Aujourd'hui, l'OSINT est reconnue par beaucoup comme une source d'information indispensable. La discussion amorcée dans de nombreux services gouvernementaux et services de renseignement sur la meilleure utilisation d'OSINT exprime ce changement. Le rôle précis et le potentiel d'OSINT restent cependant controversés. Les uns attribuent à OSINT un rôle clé et exigent un changement paradigmatique au sein des services secrets, avec un nouveau point fort sur les informations accessibles au public et une collaboration multisectorielle avec un grand réseau d'experts et d'entreprises privées. Les autres plaident simplement en faveur d'une adaptation du paradigme traditionnel dans le sens d'une pondération plus importante d'OSINT au sein de l'approche multidimensionnelle de la collecte de l'information.

Importance croissante d'OSINT

On entend par OSINT la collecte d'informations généralement accessibles au public et leur préparation en produit doté d'une plus-value pour les services secrets. L'accès aux sources utilisées peut être gratuit ou payant. Les informations peuvent provenir des médias, de services publics, de think tanks, d'universités, d'organisations non gouvernementales (ONG) ou du secteur privé.

Trois facteurs principaux ont contribué à l'accroissement de l'intérêt suscité par OSINT. Le premier se rapporte à l'élargissement considérable du spectre des menaces sécuritaires ces vingt dernières années. A l'époque de la guerre froide, les services de renseignement étaient préoccupés par un nombre restreint de défis qui avaient principalement trait aux Etats. Leur tâche cardinale consistait à découvrir les capacités et les intentions de l'Union soviétique et du Pacte de Varsovie. Depuis la chute du mur de Berlin, le domaine thématique dont s'occupent les services secrets s'est cependant dramatiquement étendu. Il englobe aujourd'hui, entre autres, le terrorisme, la prolifération des armes de destruction massive, le crime organisé, les conflits intraétatiques, les crises régionales, la migration illégale et la sécurité énergétique. Des thèmes comme le transport, les aliments, l'eau et le climat étant eux aussi de plus en plus observés sous des angles sécuritaires, le nombre de services gouvernementaux nécessitant des renseignements augmente rapidement. La valorisation d'OSINT a augmenté proportionnellement à la demande croissante d'informations dans un champ thématique étendu.

Le second facteur concerne la technologie. La révolution de l'information a fortement

© 2008 Center for Security Studies (CSS), ETH Zurich

modifié le milieu du renseignement. Elle a entraîné une plus grande transparence du monde et la mise à la disposition des services secrets d'une abondance d'informations et d'un vaste spectre de sources. Elle a aussi, simultanément, entraîné la perte du monopole des services de renseignement traditionnels sur les aptitudes et les informations nécessaires pour comprendre et maîtriser les menaces sécuritaires. Google Earth fournit aujourd'hui plus de données d'intelligence géoréférencées que la plupart des gouvernements avaient à leur disposition il y a quelques années encore. Les services secrets ont de plus en plus recours à d'autres services Internet tels que Wikipédia. Il existe en outre un marché croissant de l'information et de l'intelligence commerciales avec des services longtemps réservés au secteur public.

Les manquements des services de renseignement dans le contexte des attentats terroristes de 9/11 et de la guerre en Irak sont le troisième facteur qui a favorisé la montée d'OSINT. Surtout aux Etats-Unis, la défaillance des services secrets a été l'occasion d'un réexamen approfondi de la manière dont les informations sont recueillies, analysées et utilisées dans le cadre de la prise de décision. Plusieurs commissions ayant exigé qu'OSINT soit dorénavant utilisée plus systématiquement, le *US Director of National Intelligence* a finalement inauguré en novembre 2005 un *Open Source Center*. Depuis, le nombre d'unités OSINT a augmenté dans les instances gouvernementales américaines. Le débat autour d'OSINT s'est parallèlement intensifié dans d'autres pays, surtout en Europe.

Atouts d'OSINT

Obtenir des renseignements par le biais de sources ouvertes est moins coûteux que d'autres processus, ce qui constitue un avantage important de l'OSINT. Les informations accessibles au public peuvent en outre être recueillies par un cercle d'analystes et d'utilisateurs potentiels beaucoup plus grand étant donné qu'il ne s'agit pas d'une activité requérant des conditions légales particulières. Les informations publiques sont accessibles et évaluables 24 heures sur 24. Leur transmission est en outre moins compliquée que celle des informations classifiées.

Du point de vue des services de renseignement classiques, OSINT facilite la transmission et la publication de résultats dont la pertinence est vérifiée en s'appuyant généralement de facto sur des informations classifiées. Du point de vue d'un cercle d'utilisateurs beaucoup plus large, l'atout principal d'OSINT se situe cependant plutôt dans l'interprétation du contexte, crucial pour comprendre les questions de sécurité mondiale actuelles. Etant donné la complexité et l'interdépendance croissantes du monde, l'aptitude à identifier les problèmes qui s'ébauchent et les tendances à long terme prendra plus d'importance. Les sources indispensables à une détection stratégique précoce ne seront en règle générale pas classifiées.

Limites d'OSINT

Les partisans d'OSINT arguent que les informations accessibles au public peuvent couvrir 80 à 95 pour cent des besoins actuels des services de renseignement. L'utilisation d'informations provenant de sources ouvertes à des fins de renseignement a cependant elle aussi des limites. Il est difficile et fastidieux de filtrer parmi toutes les informations les renseignements effectivement pertinents pour l'intelligence. De telles informations ne peuvent souvent être vérifiées et questionnées qu'avec des outils de renseignement traditionnels. Le fait que la même information soit reproduite dans différents médias n'augmente pas sa réalité ni sa substance. En ce qui concerne les systèmes de gestion de l'information en particulier offerts par des acteurs privés, ils ne peuvent pas réduire les grandes dépenses analytiques nécessaires pour classer et évaluer les informations provenant de sources ouvertes.

Outre le contrôle de la qualité, la seconde faiblesse des informations provenant de sources ouvertes réside dans le fait qu'OSINT ne fournit qu'un nombre restreint des données convertibles sur le plan opérationnel. OSINT peut beaucoup contribuer à mieux comprendre les motifs d'al-Kaida, mais ne fournira pas pour cela l'endroit précis où se trouve Osama ben Laden. Les organismes terroristes et le crime organisé sont de plus en plus conscients de l'«empreinte numérique» qui les trahit et se voient forcés de se mettre hors ligne et d'opérer sous l'horizon radar. De la même manière, OSINT ne peut guère saisir toutes les informations importantes sur le programme atomique iranien ou les futurs desseins nucléaires de la Corée du Nord. Il en va de même pour les aspects opérationnels du blanchiment de l'argent ou du trafic de la drogue, pour citer deux autres exemples.

Des besoins différents

On peut tirer de l'analyse ci-dessus deux conclusions centrales. Premièrement, une utilisation stratégique renforcée d'OSINT semble nécessaire, faisable et prometteuse. Deuxièmement, l'importance de cette constatation variera d'un cercle d'utilisateurs à un autre. Le point de vue de l'observateur détermine dans une large mesure si OSINT représente un nouveau paradigme pour les services secrets ou simplement une modification du paradigme traditionnel. Pour les cercles de renseignement traditionnels, OSINT restera une méthode de collecte parmi d'autres qui complète judicieusement HUMINT, SIGINT et IMINT et devrait imprégner encore plus ces approches à l'avenir. Mais, pour de nombreuses autres instances gouvernementales, OSINT est la seule et unique «INT» à laquelle elles ont un accès intégral. C'est pourquoi OSINT peut constituer pour elles une aide décisionnelle stratégique centrale.

OSINT: Sites Web utiles

Les sites Web suivants proposent aux personnes s'intéressant à la politique étrangère et à la politique de sécurité une abondance d'informations provenant de sources ouvertes.

- **International Relations and Security Network (www.isn.ethz.ch)**
  L'ISN du Center for Security Studies (ETH de Zurich) recueille et gère dans sa base de données numériques des informations de nombreux think tanks, instituts de recherche, organismes internationaux et instances gouvernementales. Il propose une analyse quotidienne du renseignement (Security Watch) et indexe le contenu de nombreux sites Web pertinents d'un point de vue sécuritaire.
- **Oxford Analytica (www.oxan.com)**
  Un service d'analyse et de conseil stratégiques de première classe travaillant avec un réseau de chercheurs et de membres de la faculté d'Oxford et d'autres grandes universités dans le monde entier.
- **Silobreaker (www.silobreaker.com)**
  Un service de collecte de renseignement novateur qui obtient ses informations de plus de 10 000 sources différentes, y compris des blogs et des sites Web de recherche et multimédias. Silobreaker propose aussi des analyses de réseaux sociaux et des profils de personnages politiques et autres acteurs.

© 2008 Center for Security Studies (CSS), ETH Zurich

Les défis qui se posent concernant une utilisation plus systématique d'OSINT varient eux aussi d'un service gouvernemental à l'autre à l'instar de cette différenciation. Un changement de mentalité est surtout indispensable au sein des services de renseignement traditionnels. De nombreux analystes ont encore toujours des préjugés par rapport aux sources ouvertes. Cette méfiance peut aller loin, comme par exemple munir routinièrement les informations provenant de sources ouvertes du tampon «secret» et les garder sous clé, ce qui réduit leur utilité. Il y a des services secrets occidentaux qui interdisent l'accès à Internet à leurs collaborateurs pour des raisons de sécurité. En plus de ce changement de mentalité, il faudra aussi des ressources financières supplémentaires. Un renforcement des capacités d'OSINT exige des investissements tant dans la formation des analystes que dans le domaine informatique.

Le défi central des services gouvernementaux non rattachés au secteur du renseignement consiste à éviter des solutions spécifiques à certains bureaux ou départements qui entraînent des redondances et un système peu coordonné de contrats d'externalisation et d'accords de partenariat. L'élaboration d'une stratégie OSINT nationale serait utile dans ce contexte. Cette stratégie pourrait répondre à des questions fondamentales telles que: quelle solution institutionnelle tient le mieux compte des besoins des différents services gouvernementaux en OSINT? Comment peut-on améliorer le flux d'informations et la coopération entre les services gouvernementaux? Où trouver du personnel capable de penser et de travailler de manière interdisciplinaire? Comment s'y prendre avec le développement technologique rapide?

Avantages d'un centre OSINT

Chaque gouvernement doit trouver ses propres réponses à ces questions. Eriger un centre OSINT servant d'organe compétent pour les informations provenant de sources ouvertes et chargé de fournir de l'OSINT aux offices et départements intéressés pourrait être une mesure utile. Une telle unité pourrait être mise sur pied soit dans le cadre des structures de sécurité nationales existantes soit en tant qu'organisation séparée. Dans les deux cas, elle devrait cependant être soustraite à l'influence directe d'un département individuel.

Un centre OSINT pourrait s'occuper des tâches principales suivantes: soutien tant des services de renseignement traditionnels que d'autres services gouvernementaux par des recherches OSINT; coordination des besoins en OSINT à l'échelle du gouvernement; définition des instruments et technologies OSINT adéquats; coopération avec des acteurs non gouvernementaux; communication des *Best Practices* pour la collecte, la gestion, l'évaluation et la propagation des informations; entraînement et formation; alerte précoce et pronostics à long terme.

Un centre OSINT devrait disposer tant d'un état-major permanent que d'une alternance de collaborateurs de différents services gouvernementaux. L'échange et la coopération avec des partenaires du secteur privé et du secteur scientifique sont en outre indispensables. La mise sur pied et l'entretien d'une telle autorité sont certes liés à des dépenses. Mais l'accès coordonné à des services d'information de première classe et les synergies dans le domaine informatique permettront d'économiser des coûts considérables par rapport à des solutions individuelles.

OSINT en Suisse

Une série d'initiatives et de mesures indique qu'OSINT est aussi devenue un thème en Suisse. C'est ainsi qu'il existe un groupe de travail OSINT interdépartemental mettant en lumière les possibilités de synergie entre les offices concernés. Un second groupe de travail s'occupe d'OSINT au niveau du DDPS. OSINT a également été institutionnalisée dans le Service de renseignement stratégique et dans le Service de renseignement militaire tout comme dans le service de renseignement intérieur de l'Office fédéral de la police où une petite section OSINT a été créée en 2001. Différents départements ont en outre fait leurs premières expériences – mixtes – avec des systèmes informatiques de gestion du savoir.

La formulation d'une stratégie OSINT coordonnant ces activités au niveau politique, définissant les rôles et responsabilités et donnant éventuellement lieu à la création d'une infrastructure OSINT centralisée pour tous les offices intéressés se fait attendre. Il faudrait profiter des discussions actuelles concernant une révision des services de renseignement civils et la création d'un département de la sécurité pour examiner de manière approfondie et éclaircir aussi la question du rôle futur et de l'ancrage institutionnel d'OSINT en Suisse.

L'institutionnalisation d'OSINT: le modèle des Etats-Unis

Assistant Deputy Director of National Intelligence for Open Source

- Développe et surveille le concept OSINT national
- Garantit le développement d'une architecture OSINT uniforme
- Conseille les services gouvernementaux ne dépendant pas des services secrets en ce qui concerne la collecte d'informations provenant de sources ouvertes

National Open Source Committee

- Groupe de coordination de toutes les questions concernant OSINT
- Les membres sont des fonctionnaires haut placés de l'Open Source Center, de l'Office of the Under Secretary of Defense for Intelligence, du Department of Homeland Security, de la CIA, de la National Security Agency, de la National Geospatial-Intelligence Agency, du Department of State's Bureau of Intelligence and Research, de la Defense Intelligence Agency, du Federal Bureau of Investigation, etc.

Open Source Center

- Créé en 2005 par le Director of National Intelligence; la CIA sert d'organe exécutif
- Plusieurs centaines d'employés à plein temps
- Soutient les services de renseignement dans l'utilisation d'OSINT; aide à développer de petits centres OSINT au sein des offices respectifs
- Promeut la collecte, l'analyse et la propagation d'OSINT dans tous les services gouvernementaux
- Met à la disposition des fonctionnaires gouvernementaux des rapports, des traductions et des produits analytiques en ligne sur un site Web sécurisé (www.opensource.gov)

Sources: Intelligence Community Directive No. 301; CRS Report for Congress, 5 decembre 2007.

- Editeur responsable: Daniel Möckli analysen@sipo.gess.ethz.ch
- Commande d'analyses et abonnement gratuit: www.ssn.ethz.ch

© 2008 Center for Security Studies (CSS), ETH Zurich