De l'écran aux champs de bataille

Marina de CASTRO
Attachée d'administration
Ministère de l'Intérieur
Advisor du CyberCercle

Julien TOMEK
Fonctionnaire
Ministère de l'Intérieur
Service National
de Police Scientifique

L'avènement de l'ère numérique a entraîné une profonde mutation de la nature de la guerre. Les champs immatériels sont devenus le corolaire incontournable de l'affrontement terrestre, aérien et maritime. Il est aujourd'hui impossible d'envisager un conflit sans prendre en compte l'Open Source Intelligence (OSINT).

L'OSINT englobe toutes les sources d'informations ouvertes au public. Le SOCMINT (Social Media Intelligence), désigne la veille, la collecte et l'analyse de données en masse sur les réseaux sociaux, de Facebook à Twitter en passant par Instagram et bien sûr, TikTok. Suscitant déjà l'intérêt des publicitaires par le biais de tendances, de mots-clés et de hashtags, les réseaux sociaux sont devenus un terrain propice à la collecte d'information. Cartographiées et synthétisées, les tendances détectées permettent aux services de renseignement d'anticiper des crises, d'identifier des adversaires et entrent également en considération dans la planification des opérations.

Cet article s'attache à dresser un état des lieux de l'extension du domaine de la guerre aux champs immatériels, en se focalisant sur l'OSINT et le SOCMINT.

L'OSINT et la guerre

Ce qui est désigné par OSINT (renseignement en source ouverte) est en réalité un concept aussi vieux que la guerre elle-même. Bien avant l'avènement du numérique, la collecte d'information par le biais de canaux ouverts au public était un outil stratégique de premier ordre. Durant la guerre d'indépendance des Etats-Unis (1775-1783), les rebelles américains s'appuyaient sur les journaux pour connaître les mouvements des troupes britanniques. Ils pouvaient savoir rapidement dans quelle ville se trouvaient les redcoats et ainsi retracer leurs itinéraires. Ces éléments permettaient ensuite la planification d'embuscades ou de contre-attaques.

Il ne s'agit là que d'un exemple, et faire la liste complète des occurrences historiques de recours au renseignement en source ouverte nécessiterait un article entier. Cependant, il met parfaitement en lumière le fait que l'utilisation de l'OSINT n'est pas une invention récente. Ce qui en revanche constitue la spécificité du XXIème siècle est bien l'avènement de l'ère du numérique. Les conflits ont changé en profondeur et, avec eux, l'OSINT a franchi un cap, que ce soit par son aspect massif ou ses multiples modes d'utilisation.

L'invasion de l'Ukraine par les forces russes en février 2022 a fourni la preuve de l'enjeu majeur que constitue l'OSINT dans la conflictualité moderne, et surtout de son caractère incontournable dans l'anticipation des conflits. C'est pendant la phase préalable à l'offensive russe que les sources ouvertes (vidéos sur les réseaux sociaux, images satellites via

Document publié le 02/06/2023 – L'utilisation de tout ou partie de ce texte doit être soumise à autorisation ©CyberCercle

Google Maps) ont dévoilé l'étendue de la manœuvre. Dès janvier 2022, le Center for Strategic and International Studies s'appuie sur des images satellites pour développer son analyse et présenter le plan d'invasion potentiel des forces russes, avec les axes de pénétration et les objectifs poursuivis. Sur les réseaux sociaux comme TikTok, les vidéos des déplacements se multipliaient. Elles montraient des mouvements de troupes ou des passages de convois militaires.

Cette utilisation massive de l'OSINT a continué après l'offensive elle-même. Des canaux Telegram accessibles à tous permettent, aujourd'hui encore, de suivre quasiment heure par heure les combats. Ces sources sont un moyen pour les deux belligérants d'anticiper les mouvements ennemis, de planifier des attaques mais aussi de faire de la propagande en montrant leurs succès, leurs prisonniers ou les exactions (prétendues ou avérées) de l'adversaire. Les acteurs non-belligérants (Etats-Unis, Union Européenne, Chine…) en tirent également profit pour leurs propres narratifs.

En dehors du cadre strictement tactique, le conflit russo-ukrainien a montré de nombreuses possibilités d'utilisation de l'OSINT :
- évaluation des dommages sur une zone à risques ou sensible, comme cela a été le cas avec la centrale nucléaire de Zaporijjia ;
- identification d'acteurs d'influence via les réseaux sociaux (propagande en faveur de l'un ou l'autre des belligérants sur des plateformes vidéos comme YouTube entre autres).

L'émergence du SOCMINT

Les réseaux sociaux constituent une mine d'informations qui peut être très utile aux entreprises, aux institutions et aussi aux services de renseignement. En effet, dans des situations de crise ou de guerre, ils peuvent aider à la compréhension des narratifs en présence. Les commentaires, photos et autres vidéos mises en ligne par les belligérants ou leurs partisans sont autant d'informations qui peuvent être exploitées dans les manœuvres d'influence des parties au conflit. De plus, ces dernières années, les réseaux sociaux avaient été utilisés par de nombreuses organisations terroristes pour lever des fonds, recruter ou diffuser de la propagande poussant les services de renseignement à s'intéresser à ces nouveaux supports de diffusion de l'information.

Le SOCMINT concerne toute l'information disponible sur les réseaux sociaux et les outils utilisés pour analyser ces données. Le terme est né en 2012 de David Omand, Jamie Bartlett et Carl Miller. Dans le cadre de recherches pour le Centre d'Analyse des Médias Sociaux (CASM), ils ont démontré la nécessité de développer une nouvelle forme de renseignement à partir de l'information disponible sur les réseaux sociaux. Cette discipline à part entière est pleinement intégrée à l'écosystème de l'OSINT. Il ne suffit plus de compter le nombre de likes d'une publication pour en donner la tendance. Le SOCMINT va bien au-delà de la simple veille ou collecte de données en ligne. Il s'intègre tout à fait au cycle classique du renseignement et peut être considéré comme une source d'information au même titre que d'autres piliers du Renseignement comme le ROHUM (renseignement d'origine humaine), le ROEM (renseignement d'origine électromagnétique) ou le ROIM (renseignement d'origine image). Le SOCMINT n'est autre que le renseignement d'origine réseaux sociaux.

Le cycle du renseignement se construit autour de quatre axes : l'orientation du besoin en renseignement, la collecte d'information, l'analyse et la diffusion du renseignement. Quelle que soit la source, le cycle débute toujours par la connaissance des intentions du chef, de l'effet final recherché et plus précisément de ses besoins critiques en information.

Document publié le 02/06/2023 – L'utilisation de tout ou partie de ce texte doit être soumise à autorisation ©CyberCercle

S'agissant du SOCMINT, la collecte est généralement automatisée à l'aide de scripts se connectant directement aux API (Application Programing Interface) des divers réseaux sociaux. Si elle peut être facilitée sur des plateformes telles que Twitter, elle est beaucoup plus complexe sur Facebook par exemple ou d'autres réseaux sociaux étrangers comme le russe VKontakte ou le chinois Weibo. Ces derniers ont en effet mis en place des restrictions d'accès de plus en plus exigeantes. La question du stockage de ces grands volumes de données, du nettoyage et du traitement de ces dataset sont également des paramètres à prendre en considération.

L'analyse de l'information ainsi collectée peut s'appuyer sur de nombreux outils comme les schémas relationnels, les diagrammes d'influence, les réseaux de neurones formels ou encore le sentiment analysis entre autres. Une fois analysée, cette information devient un renseignement qui peut aider à cerner des opinions publiques, détecter des tendances, prévoir des comportements et même anticiper de futures menaces. L'utilisation de réseaux de neurones formels dans l'analyse de l'information issue des réseaux sociaux a gagné en popularité en raison de leur capacité à interpréter de grands volumes de données non structurées. Ils peuvent dans le même temps traiter du texte, des images, des vidéos ou du son. Il s'agit d'un modèle d'apprentissage de la machine qui s'inspire du fonctionnement du cerveau humain.

Pour conclure, l'avenir de l'OSINT et par conséquent du SOCMINT sera fortement touché par des considérations stratégiques, techniques mais aussi éthiques. La prolifération des plateformes d'intermédiation sociale et les progrès de l'intelligence artificielle permettront de traiter de plus grands volumes de données plus rapidement et plus précisément. L'OSINT, le SOCMINT et toutes autres sources de renseignement devront être de plus en plus combinées pour aboutir à un simbleautage efficace. Une telle complémentarité permettrait ainsi de mieux lutter contre la désinformation en ligne, la manipulation de l'opinion publique ou encore les cybermenaces. Enfin, la dimension éthique sera un enjeu de développement de ces outils d'analyse notamment pour ce qui concerne le stockage, la collecte et l'utilisation des données personnelles.

Document publié le 02/06/2023 – L'utilisation de tout ou partie de ce texte doit être soumise à autorisation ©CyberCercle