Drones et renseignement

Autor(en): **Rieutord, Dylan**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2018)**

Heft 2

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-823345

Robot de reconnaissance *Packbot*, http://static.progressivemediagroup.com/uploads/imagelibrary/nri/army/projects/irobot/irobot-510-packbot.

Drones

Drones et renseignement

Dylan Rieutord
Chercheur en robotique militaire et systèmes d'armes autonomes, Armée de Terre française

Le renseignement n'est plus une activité taboue. Nécessairement discret, c'est un enjeu capital dans notre monde contemporain,[1] en toutes circonstances et tous milieux. Modernisé et systématisé depuis la première guerre du Golfe,[2] nous voudrions aborder le sujet sous un angle différent. Le renseignement aérien via l'utilisation des drones est une problématique actuelle mais très fournie en documentation.[3] Le renseignement militaire de théâtre via l'utilisation de robots (à entendre comme une plateforme terrestre) l'est moins. Dès lors, les robots peuvent-ils être des agents de renseignement ou simplement des capteurs recueillant des informations ?

Si l'on entend le renseignement selon sa définition première, c'est un processus que l'on peut diviser en quatre étapes: savoir ce que l'on cherche, prendre l'information et la recouper avec d'autres sources, analyser l'information pour en faire un renseignement, le diffuser au leader pour l'exploitation. C'est précisément ce que font les unités spécialisées comme par exemple le 13e Régiment de Dragons Parachutistes en France où il est un *« Système complet de renseignement, il assure la recherche, le traitement et la diffusion du renseignement.»*[4] Nous savons qu'il est impossible actuellement pour un drone de traiter l'information qu'il recueille. Utilisé pour les missions *ISR, intelligence, surveillance and reconnaissance*, les robots terrestres peuvent être les autres capteurs permettant au moins le recoupement de sources en accord avec la numérisation du champ de bataille.

Tout comme les unités humaines, l'efficacité du renseignement réside dans la complémentarité et la synergie entre les membres d'un groupe, d'une section, d'une unité etc. Nous pensons donc qu'il serait bien plus efficace de toujours coupler les capteurs. Il convient ensuite d'adapter le dispositif en fonction du renseignement voulu et recherché. Un simple robot de reconnaissance type Packbot est suffisant pour déterminer la présence d'explosif dans un bâtiment. Un micro drone comme le *Black Hornet* britannique utilisé en Afghanistan[5] suffit pour connaître la position d'un personnel. Mais la connaissance et l'anticipation qu'ils permettent seuls, est limitée.

Une spécificité intéressante du robot terrestre capteur réside dans sa nature même. S'il venait à être capturé, la prise du dit otage n'aurait aucun impact. Et il ne serait pas soumis à la torture. L'implantation d'une forme de boîte noire et d'un système d'autodestruction est en revanche nécessaire pour tous robots.

Le renseignement est une activité discrète sinon furtive. C'est pourquoi la plupart des robots terrestres qui sont pensés pour la reconnaissance ou l'éclairage doivent allier légèreté et furtivité. L'énergie électrique sur batterie pour des missions courtes, ou les moteurs électriques pour des missions en profondeur devraient donc être privilégiés afin de minimiser la signature thermique et le bruit de fonctionnement du robot.

Des chercheurs chinois travaillent actuellement sur un camouflage électrique permettant non plus la furtivité mais bien l'invisibilité.[6] Conforme à la doctrine

1 La France a en effet porté la « connaissance et l'anticipation » comme fonctions stratégiques dans les *livres blancs* de 2008 et 2013.

2 Le renseignement a été un des centres de gravité de la Révolution des Affaires Militaires dans les années 1990.

3 Voir par exemple Noël, Jean-Christophe, « Occuper sans envahir: drones aériens et stratégie, » *Politique étrangère*, 2013/3 (Automne), p. 105-117.

4 https://www.defense.gouv.fr/terre/l-armee-de-terre/le-niveau-divisionnaire/commandement-des-forces-speciales-terre/13e-regiment-de-dragons-parachutistes

5 « Mini-Drones: Tactical ISR and Beyond, » *FuturTech*, Vol.14, Hiver-Printemps 2015, p.26.

6 « Une équipe de l'université de Wuhan, en Chine, a mis au point un robot qui change de couleur en fonction de son environnement, »*Slate*, 8 février 2016, Disponible en ligne: http://www.slate.fr/story/113783/universite-robot-cameleon, Consulté le 21 Janvier 2018.

Black Hornet, https://upload.wikimedia.org/wikipedia/commons/thumb/e/ed/Black_Hornet_Nano_Helicopter_UAV.jpg/1200px-Black_Hornet_Nano_Helicopter_UAV.

stratégique chinoise des *«Three no's,»*[7] *«nobody»* (les armes inhabitées comme les drones ou les robots), *«no-see,»* (invisibles, un cran qualitatif supérieur à la furtivité), *«no-hear»* (et silencieuses, comme les armes infrason pour créer la surprise psychologique), une fracture technologique pourrait être visible dans le cas d'une application efficiente de cette technologie dans le domaine militaire.

Si nous attendons des robots qu'ils soient des uniques capteurs, nous dirons qu'ils sont prêts. Le balisage d'une zone ou de points d'intérêts est déjà possible, et nous pourrions même envisager la spore, autrement dit le robot capteur enterré ou soigneusement placé à des endroits de collecte d'information, comme étant lui-même un relai permettant d'étendre la couverture réseau en cas de terrain difficile. Les capteurs qui seraient principalement des caméras permettraient de diffuser l'information en continue dans un mode «veille» via les *data links* au poste de commandement. C'est finalement ce que fait déjà la tourelle DODAAM's *Super aEgis* II qui a succédé à la SGR-A1 à la frontière coréenne pour sanctuariser la frontière.

7 Thomas, Timothy, «Strategic Landpower: The View from China,» *Special Essay, FMSO OE Watch*, Volume 6, Issue 3, Mars 2016, p.66.

Tourelle DODAAM's *Super aEgis* II, https://www.singularityweblog.com/wp-content/uploads/2012/10/Super_aEgis_II

Si nous attendons de ces petits agents de métal un début d'analyse de l'information recueillie, deux points sont à perfectionner. L'un touche à l'intelligence artificielle, l'autre à la transmission des données et au traitement du data. L'incorporation d'un cloud serait vraiment utile, en mettant à jour en permanence les données «blanches,»[8] le capteur qui serait en train de collecter des informations «grises» ou «noires» pourraient lui-même en faire la synthèse. Dans l'état actuel des choses, il semble impossible d'atteindre ce niveau dans le processus du renseignement robotique.

La plupart des capteurs ne comprennent pas les informations qu'ils captent. Un programme d'intelligence artificielle pourrait apporter un début de solution à cette limite, l'*Artificial Neural Network* est une technologie qui permet de traduire dans un langage naturel ce qui apparait sur une image. Permettant ainsi une identification des cibles, et générant une forme de conscience de l'environnement dans lequel doit opérer le capteur. Cette technologie couplée à la télédétection laser ou LIDAR, permettrait une autonomie totale dans la navigation, et l'identification de l'information recherchée. Plus performant que les caméras, le LIDAR est actuellement utilisé dans les voitures civiles dites autonomes. Ces technologies participeraient de la volonté d'automatisation des systèmes d'armes robotiques en délestant l'opérateur qui téléopère aujourd'hui la plupart des robots de reconnaissance.

A l'instar du Themis estonien,[9] de nombreux robots sont incapables de collecter l'information en mouvement. Mais il ne faut pas attendre que ces limites techniques soient surpassées pour penser à résoudre l'autre limite principale dans le domaine du renseignement. Si les flux de données sont multipliés, la bande passante devra être augmentée en conséquence, au risque de créer le «vertige informationnel» et de déplacer le chaos de la guerre du champ de bataille à des centaines ou milliers de kilomètres où seront en poste les analystes et opérateurs. D'où l'enjeu de perfectionner l'outil qu'est l'intelligence artificielle.

Quelle confiance accorder à des informations recueillies par les robots? Le discernement humain et la réflexion seront irremplaçables. Lors des premières interventions l'Homme devra nécessairement «baby-sitter» les robots en charge de la collecte. Avec le temps, l'Homme analyste et interprète, ne devra pas être remplacé par l'intelligence artificielle qui calculera des probabilités en fonction de variables et d'éléments lui permettant de simuler des scénarios possibles, même si cela fait partie du processus global. L'utilisation d'autres outils pour faciliter son travail comme la technologie GEOINT qui pourrait être injectée directement dans le robot est en revanche tout à fait envisageable. L'analyste devra, après avoir réalisé

8 Il s'agit d'informations ouvertes et publiques. A la différence des informations grises que l'on peut avoir de manière indirecte ou détournée. Les informations noires sont confidentielles, leur obtention revient à de l'espionnage.

9 https://www.army-technology.com/projects/themis-hybrid-unmanned-ground-vehicle/

son travail, se servir de l'IA comme d'un outil pour être sûr de n'avoir pas omis une possibilité importante dans l'interprétation des informations. De plus, si les robots peuvent prêter main forte dans les domaines du ROEM et du ROIM, le ROHUM[10] restera l'affaire de soldat de chair et de sang.

Pour autant, l'utilisation de capteurs possédant des traducteurs incorporés pourraient compenser le déficit de spécialistes dans des dialectes difficiles ou peu enseignés. La couverture géographique rendue ainsi possible ne serait pas négligeable, même si l'information restera à vérifier, à recouper, ce sera toujours mieux que rien. Rappelons également la plus-value de capteurs non humains en zone « sale.»[11]

En conclusion, les robots terrestres qui ont été conçus pour le renseignement sont actuellement des capteurs. Très utiles ponctuellement pour répondre aux menaces contemporaines, ils sont pris dans la montée en force du secteur global du renseignement et sont amenés à devenir des agents de renseignement à part entière avec des avantages et des inconvénients en comparaison de l'agent humain. Pour autant, il reste que la synergie des deux prévaut pour une efficience maximum. Des écueils sont à éviter, la dépendance vis-à-vis de l'information, la superficialité des informations recueillies, et la place de l'IA dans l'interprétation et la production de renseignement. « Occuper sans envahir » devient possible en multi domaines, présentant des avantages certains en matière d'anticipation et de connaissance mais posant toujours les mêmes questions éthiques. Il conviendra de soulever dans un prochain article la nécessaire protection des data links afin de ne pas être victime, non pas d'un transfuge à l'instar d'un capteur humain, mais d'un détournement ou d'un piratage de données induisant une faute tactique, ayant elle-même de possibles répercussions au niveau stratégique. Attention donc au « général tactique »[12] qui ne doit pas se laisser prendre par « l'effet tunnel » induit par l'afflux de données.

D. R.

10 Renseignement d'origine électromagnétique, renseignement d'origine image, renseignement d'origine humaine

11 A entendre comme contaminée par des attaques chimiques, biologiques, voire nucléaires.

12 Voir la notion de « caporal stratégique » dans, P.W Singer, Wired for War, Pinguin Press, New-York, 2009. Le général tactique est le fait de s'intéresser aux plus petits détails du terrain alors qu'on est en poste pour mener l'opération avec la plus grande acuité possible.

Renseignement

Un « mouchard » et l'indispensable secret des opérations militaires

L'application Strava, compatible avec de nombreuses montres connectées et permettant de mémoriser, d'échanger et de visualiser les performances physiques en temps réel, a connu un grand engouement au sein de la communauté militaire internationale.

L'émotion suscitée, au début février 2018, en raison des risques de sécurité liés au mode de cartographie en ligne fusionnant les treize mille milliards de coordonnées GPS collectées auprès des utilisateurs, a créé un vent de panique au sein des services de sécurité. Il touchait au niveau d'activités de certaines installations militaires, aux itinéraires utilisés lors des patrouilles et leurs fréquences, les zones réservées. On a interdit l'utilisation de l'application. Cette information a tout du réchauffé, cette carte étant disponible et exploitée par les experts du renseignement depuis plusieurs années.

Quelles informations inédites peut-on exploiter sur *Strava*? Sans recourir à des outils complémentaires, cette cartographie a pu livrer d'emblée la localisation de plusieurs FOB en Afghanistan, les transits sur la base russe de Kuzminsky à la frontière ukrainienne, le centre de commandement sol-air taïwanais, la batterie de missiles émiratie Patriot au Yémen. Couplée à *Google Earth*, *Strava* est donc un moyen puissant pour identifier le niveau d'activité des sites militaires sensibles, qui se distinguent la plupart du temps à l'image par la présence de périmètres de sécurité.

L'enrichissement des cartes par des données de terrain issues de la communauté des utilisateurs de Wikimapia ou d'Openstreetmap permet d'aller encore plus loin et d'identifier les gisements d'activités dans les zones désertiques, comme la sécurisation des pipelines en Syrie, les détours utilisés par les trafiquants, les circuits des tour-opérateurs... *Strava* permet aussi de révéler certains paradoxes. Ainsi aucun personnel militaire ne semble autorisé à pénétrer dans le camp 7 de Guantanamo, qui reste interdit aux rapporteurs de l'ONU et où sont détenus les djihadistes à plus « haute valeur (...). Les coordonnées GPS collectées à proximité de certains sites moscovites sensibles (Kremlin, aéroport Vnukovo...) sont sans rapport avec la réalité et démontrent l'efficacité des dispositifs de brouillage GPS mis en place par les autorités russes.

En somme, les ressources ouvertes de *Strava* permettent d'imaginer les fonctionnalités offertes par les *malwares* commerciaux, qui permettent de suivre simultanément plusieurs dizaines de milliers d'individus!

TTU N° 1095, 7 février 2018