Aujourd'hui, la très grande majorité des drones[1] utilise une ou plusieurs liaisons de données. Ceci est vrai aussi bien pour les drones militaires que pour les drones civils. Toutefois, des appareils peuvent techniquement aussi être mis en œuvre sans moyen de communication, de manière totalement autonome. Certains drones du commerce disposent même de la capacité de vol autonome totalement passif en reliant différents points géographiques préprogrammés.

Une liaison de données impose d'émettre et de recevoir de l'énergie électromagnétique. C'est donc quelque chose d'indiscret qui peut être intercepté et brouillé. D'ailleurs, la détection radiofréquence et le brouillage sont parmi les moyens privilégiés dans la lutte anti-drones. Toute liaison de données est, en soi, potentiellement un point faible ; c'est une des grandes vulnérabilités de nos moyens actuels, qu'ils soient civils ou militaires, due à l'hyperconnectivité de nos équipements.

En conséquence, il apparaîtrait alors pertinent de privilégier des drones qui fonctionnent de façon totalement autonome, soit en pré-programmant leur trajectoire, soit en les dotant de l'intelligence nécessaire pour évoluer en toute autonomie. Mais ce mode d'action présente lui aussi quelques inconvénients dont certains compromettent directement l'avantage apporté par les drones.

Les drones civils

Les *« dronistes »*, en général, pilotent eux-mêmes leurs engins car cela reste plus précis et répond mieux à leurs besoins (prises de vues, inspections, mesures…). La seule application où un télépilotage apparaît superflu est celle des drones livreurs dont la fonction se limite à aller d'un point A à un point B. Néanmoins, même dans ce cas, la sécurité impose que ce type de drones soit doté d'un dispositif de signalement électronique, à l'image des ADS-B/IFF (système de signalement électronique des aéronefs). C'est aussi le cas des drones de surveillance dits *« autonomes »*, c'est-à-dire sans pilote humain. Mais cela ne signifie pas pour autant qu'ils évoluent sans liaisons de données. Le pilotage est effectué par la station de contrôle à laquelle le drone envoie la vidéo et la télémétrie tandis que la station lui transmet les ordres de télécommande[2] ; ces appareils ne sont donc pas réellement autonomes.

Quant aux drones civils détournés par des tiers à des fins malveillantes, l'agresseur doit nécessairement rester maître de sa machine, quelle que soit la finalité de son action. Si c'est une mission de renseignement, l'utilisateur du drone doit pouvoir piloter le drone et sa caméra afin de recueillir les informations dont il a besoin. Si le drone est utilisé à des fins d'attaque et de destruction, l'opérateur doit être en mesure d'ajuster précisément sa cible. Bien entendu, une attaque à partir des coordonnées reste possible mais cela signifie alors que l'attaquant a réussi à obtenir celles-ci par un autre moyen (*Google Earth*, par exemple), que la taille de la cible est relativement imposante pour être touchée en tenant compte de l'imprécision de la position (quelques mètres avec un guidage par satellite), et que la cible est fixe. Toutefois, détruire à partir des coordonnées une cible assez imposante, comme un bâtiment, avec un drone civil apparaît compliqué car la charge emportée reste relativement modeste. Aussi, seules des attaques symboliques peuvent être menées. Un drone peut également viser une

foule de manière aveugle, de façon à faire un maximum de victimes. Un point est néanmoins important : pour des raisons de communication, les groupes terroristes ou criminels ont souvent intérêt à diffuser les images de l'attaque à des fins de propagande ou pour la revendiquer. De ce fait, il est très probable qu'ils préféreront quand même garder un lien pour bénéficier, *a minima*, du retour vidéo.

Les drones militaires

Dans le cas d'une application militaire, un des gros avantages du drone est que son emploi permet, avec la même plateforme, d'assurer les fonctions reconnaissance, de surveillance, de détection et d'identification des cibles et, de plus en plus fréquemment, de destruction pour les drones équipés d'armements ou pour les drones suicides. L'emploi d'une télécommande est donc primordial. Pour réaliser une attaque à partir coordonnées, c'est-à-dire en utilisant un drone en vol autonome, il faut disposer d'une désignation d'objectif fournie par un autre capteur et, dans ce cas, le drone n'apporte aucune plus-value par rapport à un missile, une roquette ou un obus. De plus, les armées aussi ont besoin d'un retour vidéo pour la confirmation de la destruction et l'évaluation des dégâts ; sans compter que, parfois, ces images servent aussi pour la communication, comme le font de plus en plus souvent les armées.

https://theatrum-belli.com/wp-content/uploads/2021/06/azerbaijan-army-drone-strikes-against-armenian-army-bayraktar-tb2-israeli-harops-16-oct-2020.mp4

Impact de l'intelligence artificielle

L'arrivée de l'intelligence artificielle (IA) dans les drones pourrait permettre des attaques en mode autonome (donc sans liaisons de données), relativement précises, sans coordonnées, ni même désignation préalable d'objectif. Si l'algorithme a été entraîné à attaquer un ou plusieurs types de cibles (reconnaissance image), on peut effectivement imaginer que des drones puissent patrouiller sur des zones données et passer à l'attaque en cas de reconnaissance d'une des cibles enregistrées. Toutefois, l'IA a des limites et est encore assez facilement leurrable[2], ce qui fait que le risque d'attaque de *« fausses cibles »* est élevé, ainsi que celui de la non-reconnaissance d'une cible. A cela, il faut ajouter les risques de dommages collatéraux en cas d'erreurs ou si l'objectif se trouve au milieu d'une foule de civils, par exemple.

Malgré l'incertitude du résultat et des risques éventuels, il semble bien que la Russie et la Turquie aient décidé d'emprunter cette voie, à l'image du dernier prototype de drone KYB de la firme Kalachnikov qui, *« si ses opérateurs entraient par exemple l'image d'un véhicule militaire américain [...], pourrait rechercher ce type d'équipement sur le champ de bataille »* ou du drone turc KARGU de la société STM qui est donné pouvoir détecter, classifier et identifier de

manière autonome certaines cibles. Si de tels drones étaient effectivement utilisés de manière totalement autonome, on serait clairement face à un système SALA (Système d'Arme Létal Autonome), ce qui pose des problèmes éthiques à certaines nations, notamment aux pays européens. Les Russes et les Turcs ne sont d'ailleurs pas les seuls à s'intéresser à des solutions de ce type : l'Afrique du Sud, Israël, les Émirats arabes unis, la Chine, les États-Unis ont aussi des projets similaires.

Il est toutefois peu probable qu'à court terme l'emploi totalement autonome de ce type de drone se généralise dans les armées. Les risques d'erreurs demeurent importants et cela nuirait grandement à l'image de la nation utilisatrice. Il est bien plus probable que leur emploi ressemble davantage à celui de certains missiles (missiles de croisière SCALP ou missiles antinavires AGM-158C LRASM, par exemple) qui ont des capacités de reconnaissance de cible, mais à partir d'une position géographique ou d'une désignation d'objectif associée à une seule cible possible : la surface de recherche se trouve ainsi limitée, diminuant ainsi grandement les risques d'erreurs de reconnaissance. Même dans ce cas, il est assez probable que des liaisons de données soient maintenues — d'ailleurs, il se développe des concepts de porteurs dédiés à ce rôle —, comme sur certains missiles, pour récupérer les vidéos et surtout, pour garder la possibilité de confirmer ou d'annuler une attaque (cette fonctionnalité est clairement indiquée sur la majorité des projets de drones utilisant l'IA).

L'arrivée de l'IA n'est donc pas forcément synonyme de disparition des liaisons entre les drones et les opérateurs, mais c'est un moyen de rendre les drones bien plus résilients au brouillage, surtout dans les phases de transit. Néanmoins, il semble que ces liaisons de données resteront importantes pour les attaques dont les opérateurs garderont le contrôle, au moins pour valider la cible. Autre point très important : un drone sans aucune émission radioélectrique est aussi un drone que l'on n'identifie pas, donc que l'on risque de confondre avec un drone ennemi. *A minima*, un dispositif de signalement électronique apparaît donc nécessaire, sauf à prendre le risque de détruire ses propres drones.

Par contre, on peut imaginer que certains groupes terroristes ou criminels aient moins de réticences à utiliser ce type de technologie en autonomie totale, surtout qu'elle est déjà, en partie, disponible. Le robot de DJI RoboMaster S1 dispose d'un module IA permettant la reconnaissance d'images et de personnes. Le risque est toutefois à nuancer. C'est une chose de faire reconnaître un objet par un jouet à quelques mètres, mais c'en est une autre de faire tourner un algorithme sur des images en temps réel pour quadriller une zone de plusieurs kilomètres carrés depuis une plateforme aérienne. Cela demande une puissance de calcul importante et des compétences bien particulières pour concevoir de tels systèmes. En revanche, ce risque est plus important avec les drones terrestres ou maritimes dont les vitesses de déplacement sont potentiellement bien plus faibles et bien plus compatibles avec les temps de traitement des images des produits du commerce. De plus, ils évoluent dans un contexte où le risque d'erreur est aussi plus faible. Un petit drone terrestre qui doit attaquer un char n'aura pas trop de mal à en reconnaître un à quelques dizaines de mètres, et un drone maritime n'aura pas trop de mal à identifier un navire sur la mer.

Toutefois, il ne faut pas perdre de vue que l'IA sera un moyen assez contraignant à utiliser pour un groupe non étatique qui devra faire, en amont, le lourd travail de labellisation et

d'enrichissement de sa base de données d'apprentissage. Tout ce travail nécessite des compétences, des renseignements et une structure adaptée qui ne sont pas forcément à leur portée.

Les essaims

Les essaims de drones, dont on parle tant aujourd'hui compte tenu du nombre de projets sur le sujet, doivent coordonner le vol des différentes machines du groupe. Cela nécessite qu'elles communiquent entre elles afin d'ajuster le vol de chaque élément de l'essaim pour que celui-ci garde sa cohérence. Donc, même si on imagine une attaque avec un essaim de drones qui évoluerait de manière autonome (cas hypothétique), c'est-à-dire sans liaison entre l'essaim et un opérateur déporté, les liaisons entre les drones restent une vulnérabilité potentielle à exploiter (détection et brouillage).

* * *

Aujourd'hui la probabilité qu'un drone évolue sans liaisons de données peut être considérée comme relativement faible car les inconvénients sont largement supérieurs aux avantages. Faire évoluer un drone en totale autonomie lui retire une bonne partie de son intérêt, même s'il en a la capacité technique. Le risque apparaît d'autant plus faible qu'il est relativement simple de créer une liaison de données discrète et/ou robuste au brouillage, comme le permettent les radios logicielles (SDR). Il peut être très problématique, d'un point de vue opérationnel, d'envoyer des drones sur une zone et de n'avoir aucun retour. Il sera impossible de savoir s'ils ont trouvé des cibles, si des cibles ont été détruites ou pas, si les drones se sont fait abattre, etc. Le renseignement obtenu par les drones est lui aussi primordial et il ne peut être obtenu que si ceux-ci peuvent communiquer avec leur station de contrôle. Ceci est d'ailleurs à mettre en parallèle avec les appareils à équipages qui ont, eux aussi, des liaisons de données afin de pouvoir envoyer, en temps réel ou quasi réel, les renseignements obtenus.

Néanmoins, le risque n'est pas totalement absent à moyen/long terme sur certains drones militaires, puis dans le domaine des drones civils, sans pour autant que cela devienne systématique. En effet, cela ne répondra pas aux besoins opérationnels de C4ISTAR (*Computerized Command, Control, Communications, Intelligence, Surveillance, Target Acquisition and Reconnaissance*) des forces. Dans un monde où la rapidité de diffusion de l'information est un des socles des opérations militaires, les liaisons de données sont donc essentielles. Sauf quelques cas bien particuliers, les drones resteront connectés à leurs opérateurs car c'est bien là leur atout principal par rapport à d'autres moyens potentiellement moins chers (obus par exemple) ; et le besoin d'identification des drones rend nécessaire la présence d'un système de signalement électronique, comme pour les aéronefs pilotés. De ce fait, la détection radiofréquence et la neutralisation par brouillage resteront des moyens pertinents de détection et de neutralisation. La difficulté est, bien entendu, d'être en mesure de détecter et d'identifier les communications et les dispositifs de signalement des drones sur un spectre électromagnétique de plus en plus chargé.

Olivier DUJARDIN / CF2R

NOTES :

1. Souvent désignés par l'acronyme UAV (*Ummanned Aerial Vehicle*).
2. *« Applications de l'IA au domaine militaire, perspectives et risques »*, HS n°73 de DSI.