La menace que représentent les drones fait régulièrement la une de l'actualité, et est de plus en plus prise en compte comme menace potentielle. Pour autant, les drones recouvrent une catégorie de matériel très vaste. Cela va du drone aérien (de quelques grammes à plusieurs tonnes), en passant par les drones terrestres (quelques centaines de grammes à plusieurs tonnes) et les drones maritimes (de quelques dizaines de centimètres à plusieurs dizaines de mètres). Toutefois, les catégories supérieures de drones, les plus gros (drones MALE, HALE, blindés, robotisés ou navires autonomes), ne représentent pas forcément une menace nouvelle car elle peut être considérée comme équivalente à celle représentée par les plateformes pilotées. Cette catégorie peut donc être traitée par les moyens traditionnels (missiles anti-aériens, antichars, anti navires…).

A contrario, la catégorie la plus petite représente surtout une menace d'ordre informationnelle (renseignement) tant leur charge utile est réduite et ne représente pas forcément un danger physique. Cependant, ce dernier point pourrait être nuancé car il est toujours possible, avec quelques grammes, de réaliser une attaque chimique ou bactériologique. Néanmoins, le danger le plus grand est aujourd'hui représenté par les drones de quelques centaines de grammes à quelques dizaines de kilogrammes, qu'ils soient aériens, terrestres ou maritimes. En effet, ces plateformes, tout en restant compactes et discrètes, peuvent alors embarquer des charges militaires non négligeables. C'est à cette catégorie que nous nous intéresserons plus spécifiquement. La lutte contre ces drones est aujourd'hui un enjeu majeur mais qui reste surtout concentré sur ceux qui volent ; la menace représentée par les drones terrestres ou maritimes de petites tailles ne semble pas encore faire l'objet d'études particulières ce qui est, sans doute, une erreur.

La neutralisation des drones malveillants est toutefois un défi technique tant les menaces peuvent être variées et les contraintes différentes à chaque situation. De plus, avant de neutraliser un drone, encore faut-il être en mesure de le détecter alors que la catégorie qui représente aujourd'hui l'essentiel de la menace est, de par son encombrement, déjà naturellement discrète.

Les moyens de détection

Avant de penser à éliminer ou neutraliser une menace, il faut déjà pouvoir, non seulement la détecter, mais aussi être capable de déterminer à quoi correspond cette détection[1]. Pour ce qui concerne les drones aériens, leurs tailles sont équivalentes à celles des oiseaux. Dans le cas des drones terrestres, leurs dimensions sont proches de celle des petits mammifères et, pour les drones maritimes, il faut être en mesure de les différencier de la houle ou de tout autre objet flottant. A cette difficulté s'ajoute aussi le fait que de plus en plus de drones sont conçus sur la logique du bio mimétisme, ce qui complique encore plus la problématique de l'identification de la menace.

Drone bio-mimétique

Pour répondre à ce besoin, les industriels ont développé, ou imaginent, différentes solutions qui sont toutes plus ou moins complémentaires, avec leurs avantages et leurs inconvénients, mais qui ne sont pas, à ce jour, complètement satisfaisantes individuellement.

- **La détection RADAR :** elle permet la détection de tout temps mais ne permet pas de discriminer les oiseaux des drones. Des études sont menées pour analyser, grâce à l'IA, la cinématique des différentes détections pour repérer les drones. La limite de ce principe est que le comportement cinématique d'un oiseau est relativement facile à imiter pour un drone. L'autre moyen est l'analyse micro doppler des échos radar afin de détecter la rotation des hélices des drones. L'efficacité de ce type de traitement dépend de la matière des hélices (la réponse au radar sera différente si ce sont des hélices en carbone, en plastique ou autre), et surtout de la configuration aérodynamique du drone. C'est surtout adapté pour les drones multicoptères. L'utilisation d'un radar parait compliquée pour la détection de petits drones terrestres car il ne sera pas possible de discriminer un drone d'un petit mammifère (comme pour les détecteurs de mouvements) et ce type d'objet sera de toute façon difficile à extraire du retour du sol. Quant aux drones de surface, ils seront difficiles à discerner dès qu'il y aura un peu de houle. Si le radar offre une détection tout temps, il ne permet pas à lui seul, une classification certaine des détections.
- **La détection par radio-fréquences :** tout comme le radar elle offre l'avantage de détecter par tout temps et de relativement loin les liaisons de données utilisées par les

drones. Cette méthode est réputée pour son efficacité identique (drone aérien, terrestre ou maritime) mais son inconvénient majeur réside dans la difficulté d'obtenir avec précision[2] la position d'une source RF dès que la distance de détection augmente ; et cela ne peut fonctionner que si, d'une part, le drone utilise une liaison de données RF (ce qui n'est pas obligatoire) et d'autre part, que l'on soit en mesure de déterminer les fréquences utilisées. Ce dernier point peut être relativement ardu dans un environnement électromagnétique chargé, notamment en cas d'utilisation de moyens de transmissions difficiles à associer à un drone (GSM ou liaison satellitaire par exemple). La détection RF n'est donc pas entièrement suffisante pour assurer la détection certaine d'une menace mais se révèle toutefois assez efficace, offre un préavis de détection appréciable et est relativement économique.

- **La détection électro-optique :** c'est sans doute le moyen le moins onéreux mais peut-être aussi un de ceux qui est le plus limité. La détection se dégrade assez vite dès que la luminosité baisse et l'environnement doit rester sans brouillard ni fumées. Il est aussi difficile de discriminer un drone d'un oiseau ou d'un mammifère de loin (distance de l'identification assez faible). Un tel type de détection ne peut se suffire à lui-même sans être complété par d'autres moyens.
- **La détection Infrarouge :** elle est souvent associée aux systèmes électro-optiques. Elle a l'avantage de permettre une détection jour/nuit mais elle reste sensible aux conditions météorologiques et aérologiques. De plus, elle ne permet pas de discriminer un oiseau/mammifère d'un drone. C'est peut-être dans le milieu maritime que la détection IR serait la plus efficace car, à la surface de l'eau, il y a une probabilité beaucoup plus faible de tomber sur un mammifère marin. Là encore, ce moyen de détection ne peut se suffire à lui-même.
- **La détection sonore :** cela n'est aujourd'hui applicable que pour les drones multicoptères. Une méthode qui souffre d'une portée de détection limitée et d'une localisation relativement peu précise, surtout dans des environnements complexes comme les environnements urbains.

Si le problème de la défense anti-drone se rapproche des domaines de luttes traditionnelles (anti-aériennes, anti-navires, anti-véhicules), la menace, en considération de sa taille, est ramenée au même niveau que celle des êtres vivants dans leur milieu naturel. De fait, si les industriels se sont naturellement inspirés de ce qu'ils font déjà pour la défense sol-air, ils arrivent aujourd'hui à buter sur les limites physiques de cette menace particulière. Si conceptuellement le raisonnement est similaire, l'approche technique de la réponse doit être pensée différemment pour prendre en compte cette spécificité. Il n'existe pas aujourd'hui de moyen « *ultime* » pour détecter et surtout identifier ce type de menace, à coup sûr et à distance de sécurité. Seule une combinaison de capteurs permet d'approcher cet objectif mais certaines attaques resteront très difficiles à détecter, comme celles utilisant le bio mimétisme et n'utilisant pas de liaison de données RF par exemple.

Les moyens de neutralisation

La neutralisation de ce type de danger pose aussi un problème car, le coût du vecteur attaquant étant très faible, la réponse ne peut pas mettre en jeu des moyens trop onéreux.

Cela serait économiquement insoutenable. À l'instar du système *Iron Dome* israélien qui utilise, pour intercepter des obus ou des roquettes d'une valeur comprise entre 100 et 1 000 dollars, des missiles qui coûtent 50 000 dollars chacun. Cela disqualifie donc l'essentiel des systèmes de défense à base de missiles, même s'ils se sont avérés efficaces[3] : leurs coûts sont bien trop élevés par rapport à la menace. Partant de ce principe, plusieurs alternatives sont présentes sur le marché, chacune avec ses avantages et ses inconvénients.

- **Brouillage des liaisons radio-fréquences (RF) :** c'est un des moyens privilégiés aujourd'hui car il n'entraîne pas de destruction de la cible avec les dommages collatéraux pour les personnes et les infrastructures (chutes de débris, déclenchement de la charge militaire etc.). L'inconvénient principal de cette méthode est que cela ne peut être utilisé que pour les drones qui sont pilotés par RF, à la condition aussi que l'on ait pu identifier la ou les fréquences utilisées. Toutefois la principale limitation à ce procédé est d'ordre juridique. Pour le moment, seuls les services étatiques ont l'autorisation d'utiliser des brouilleurs en raison des risques de dommages collatéraux (brouillage sur d'autres systèmes). Le brouillage, malgré son efficacité (cela semble aujourd'hui le moyen d'action privilégié des forces russes[4]) et son faible coût, ne peut donc pas être utilisé par des acteurs privés pour défendre un site.
- **Brouillage des moyens de navigation par satellite GNSS (GPS, GALILEO, Glonass, etc.) :** il n'est efficace que si les drones utilisent ce type de moyen de navigation sans télécommande. Tout comme la technologie précédente, l'emploi de brouilleurs de GNSS est proscrit en dehors des services étatiques. Même pour les services officiels, l'emploi est très limité car, compte tenu du nombre d'applications utilisant ce procédé de localisation, les effets collatéraux peuvent être dangereux. Il y a les mêmes limitations pour le *Spoofing* (falsification de la position) des moyens GNSS et donc le cadre de son emploi est extrêmement limité. Cette méthode est très souvent associée aux solutions de brouillage des liaisons RF.
- **Laser aveuglant (Dazzling) :** le principe est d'utiliser un laser de faible puissance que l'on pointe vers les optiques du drone afin de les aveugler. Si le drone est télé piloté, cela peut faire échouer une attaque, mais encore faut-il être dans l'axe des optiques. Ce système est surtout efficace contre les risques de prises de vue illicites (espionnage, paparazzi[5]...) mais est relativement peu efficace pour déjouer une attaque. Ce système simple et peu coûteux est intéressant pour lutter contre les risques de fuites informationnelles.
- **Laser de puissance :** si l'emploi d'un Laser pour la destruction de drones est infiniment moins onéreux que l'utilisation de missiles, il n'en demeure pas moins que l'usage reste limité à des applications militaires, dans des environnements dégagés. Celui-ci n'est pas utilisable en milieu urbain (risque de dégâts collatéraux), ni à proximité de la population avec les risques inhérents à la chute des débris ou au déclenchement de la charge militaire (il faut garder à l'esprit qu'elle peut contenir des substances radiologiques, bactériologiques ou chimiques). En dehors des limitations physiques des lasers[6], cela reste une option intéressante, si l'environnement le permet, en cas d'attaque multiple, en offrant une réponse potentiellement assez rapide pour traiter plusieurs menaces.
- **Impulsion électromagnétique (IEM) :** plusieurs sociétés proposent des canons à IEM pour neutraliser les drones, l'impulsion électromagnétique ainsi générée devant neutraliser les circuits électriques et électroniques. Si le concept est séduisant sur le

papier, il apparaît bien plus délicat à mettre en application. Premièrement, la faible focalisation du faisceau et le taux d'absorption atmosphérique implique que ces armes ont une portée relativement réduite, sauf à demander une énergie très importante, ce qui en ferait des systèmes à la fois extrêmement onéreux et encombrants. Ensuite, l'ouverture angulaire relativement importante du faisceau rend impossible de cibler précisément un objectif, ce qui risque d'impliquer des dommages collatéraux, à commencer sur ses propres équipements situés à proximité. Les systèmes proposés sont donc, en l'état, délicats à utiliser en dehors d'un environnement parfaitement dégagé (désert, milieu marin…). De plus, la destruction des circuits électriques et électroniques entraînera la destruction du drone, avec le risque de chute et de déclenchement de la charge militaire. L'emploi de ce type de moyen reste également réservé aux services officiels. Par contre, l'impulsion électromagnétique constitue une réponse intéressante pour faire face à des attaques de saturation car la faible focalisation du faisceau permet justement, avec un seul tir, de traiter plusieurs menaces en simultané dans un même secteur angulaire.

- **Lance-filets :** des fusils lance-filets ont été développés afin de capturer les drones en vol. Non seulement leur portée est faible (entre 20m et 200m au maximum) ce qui fait que le drone risque d'être intercepté très (trop) proche de sa cible, mais en plus, si le drone est un peu agile, l'opérateur a toutes les chances de le rater. Or, quand on ne dispose que d'un rayon d'action de 200m au maximum, il n'y aura probablement pas de deuxième chance.

[embedyt] https://www.youtube.com/watch?v=CxeESBPBOSg[/embedyt]

Si le principe présente l'avantage de ne pas détruire le drone (descente par parachute), son efficacité reste limitée de par sa faible portée et il risque d'être inopérant face à des drones à voilure fixe ou trop gros pour le filet. Pour augmenter le rayon d'action de ce type d'effecteur, il est plus pertinent de l'embarquer sur un drone intercepteur, comme ce qui est fait avec les drones *Excipio* mais, malheureusement, ils ne peuvent tirer qu'un ou deux filets, selon le modèle, ce qui ne laisse pas le droit à l'erreur. Il faudrait réussir à diminuer l'encombrement du lance-filet de façon à garder un drone suffisamment rapide et agile pour lancer plusieurs filets dans un seul vol. Bien entendu cette méthode n'est valable que pour les drones aériens, elle serait très peu efficace contre des drones terrestres ou maritimes.

[embedyt] https://www.youtube.com/watch?v=LgWlm5zrY4w[/embedyt]

- **Drone intercepteur** : il existe deux versions du concept. La première consiste à percuter le drone en vol de façon à le détruire, avec les inconvénients que cela représente ; la seconde consiste à l'attraper dans un filet suspendu sous le drone évitant ainsi sa destruction. Dans les deux cas, l'utilisation d'un drone intercepteur requiert beaucoup de dextérité de la part du pilote du drone intercepteur qui doit être capable de venir au contact du drone malveillant si celui-ci effectue des manœuvres pour y échapper. Cela demande aussi un drone intercepteur suffisamment rapide, maniable et de bonne taille de façon à, soit pouvoir encaisser le choc, soit être capable de supporter le poids du drone intercepté.

[embedyt] https://www.youtube.com/watch?v=MrE-nrGEW20[/embedyt]

- **Destruction par moyens cinétiques :** cela recouvre le tir par arme à feu ou par jet d'eau. Quel que soit le procédé utilisé, il y a destruction du drone avec tous les risques associés (chute, déclenchement de la charge militaire). L'emploi des armes à feu étant réglementé et les risques collatéraux étant importants (le coup au but étant très loin d'être garanti), le cadre d'emploi restera très limité. En ce qui concerne la destruction par jet d'eau, c'est la faible portée du tir (quelques mètres) qui sera un inconvénient majeur. Les moyens cinétiques peuvent être une solution intéressante contre les drones terrestres ou maritimes car les distances d'engagement seront plus faibles et il n'y a pas de risque de retombées.
- ***Hacking* :** Il présente l'avantage de prendre le contrôle du drone assaillant par hacking de la télécommande. Toutefois, cela nécessite de parfaitement connaître le protocole utilisé donc d'avoir, non seulement une base de données parfaitement à jour, mais aussi d'avoir réussi à parfaitement identifier le modèle du drone. Ce procédé sera inopérant si le modèle du drone est inconnu ou si le protocole n'est pas à jour dans la base de données. De même, si le drone n'utilise pas de liaison radio-fréquences, le hacking est impossible.
- **Les Rapaces :** plusieurs expérimentations avec des rapaces ont été effectuées pour intercepter les drones. Si quelques bons résultats ont pu être obtenus ici et là, le procédé se révèle très peu fiable. En effet, selon la taille du drone, les rapaces rechignent à s'aventurer (risque de blessure avec les hélices) et surtout, les rapaces préféreront toujours aller attraper une souris comestible plutôt qu'un drone. De ce fait, cette piste est aujourd'hui pratiquement abandonnée pour la lutte anti-drone.

Qu'il s'agisse de détection ou de neutralisation, aucune des solutions aujourd'hui proposées ne permet une protection totale. Chaque solution n'est valide que pour certains cas. C'est d'ailleurs sans doute ce qui explique, en partie, le faible nombre de solutions anti-drones aujourd'hui déployées proportionnellement au nombre de site sensibles. Sans analyse des risques, les clients potentiels ont probablement beaucoup de difficultés à appréhender le niveau de la menace[7] contre laquelle ils doivent se protéger. Les solutions aujourd'hui proposées ne sont que rarement associées à un type d'attaque identifié et caractérisé, ce qui n'aide pas au choix. La situation est plus difficile pour le secteur privé car, parmi les solutions de neutralisation disponibles, beaucoup sont d'un usage réglementé et donc inaccessibles pour eux. Dans ces conditions, il ne faut pas s'étonner que le danger potentiellement représenté par les drones soit mis de côté par beaucoup d'acteurs privés. Malheureusement, on peine à voir apparaître des solutions réellement utilisables par tous, acteurs privés compris. À côté de cela, la menace posée par les drones ne fera que grossir[8] : pour s'en convaincre, il suffit de voir les essais qu'effectuent différentes armées dans le monde sur l'emploi des drones, souvent dérivés de modèles civils, que ce soit en renseignement, en attaque, en essaim[9] etc. Si aujourd'hui on peut considérer cette menace comme relativement peu évoluée, car surtout composée de drones du commerce peu ou pas modifiés (les modifications apportées ne remettent pas en cause les moyens de détection et de neutralisation aujourd'hui utilisés), c'est surtout parce qu'elle ne rencontre pratiquement aucune résistance. Dès que les premiers moyens de lutte seront déployés à une échelle significative, la menace s'adaptera aussi très vite. Si les narco trafiquants ont su mettre au point et construire des sous-marins océaniques[10] pour leurs trafics, nul doute qu'ils sauront adapter les drones en conséquence, les rendant bien plus difficiles à détecter et à neutraliser, sans même parler des machines développées

spécifiquement pour un usage militaire.

Olivier DUJARDIN

NOTES :

[1] https://cf2r.org/rta/detection-classification-identification/

[2] https://cf2r.org/rta/localiser-les-emetteurs-radio-electriques/

[3] https://www.lepoint.fr/monde/la-russie-affirme-avoir-abattu-pres-de-60-drones-en-syrie-en-2019–28-09-2019-2338295_24.php

[4] https://www.armenews.com/spip.php?page=article&id_article=70508

[5] https://www.fr24news.com/fr/a/2020/07/harry-et-meghan-poursuivent-en-justice-pour-les-photos-de-drone-de-leur-fils-archie-3.html

[6] https://cf2r.org/documentation/armes-a-energie-dirigee-possibilites-et-limitations/

[7] https://cf2r.org/rta/la-menace-des-drones/

[8] https://www.midilibre.fr/2020/10/21/un-montpellierain-arrete-avec-un-drone-et-des-explosifs-lors-dun-controle-routier-9154825.php

[9] https://jamestown.org/program/russias-armed-forces-test-uav-swarm-tactics-in-kavkaz-2020/

[10] https://www.ouest-france.fr/europe/espagne/sous-marin-transportant-de-la-drogue-en-espagne-le-troisieme-membre-de-l-equipage-ete-interpelle-6631696