À la suite de notre article sur la détection et la neutralisation des drones nous avons adressé quelques questions en lien avec l'article aux principaux acteurs français de la lutte anti-drone. Trois ont aimablement acceptés de répondre à nos questions (CERBAIR, ROBOOST et MC2 TECHNOLOGIES). Trois points de vue et trois approches différentes de ce domaine de lutte émergent mais dont l'importance ne fait que croitre à mesure que la technologie des drones se démocratise. Le sujet de la lutte anti drone est très loin d'être clôt car la menace n'a pas fini d'évoluer et présente des caractéristiques très variées.

Propos recueillis par Olivier DUJARDIN.

TB : Expliquez-nous en quoi consiste votre solution anti-drone, les choix technologiques que vous avez faits que ce soit pour la détection et la neutralisation.

CERBAIR : Les solutions conçues et produites par CERBAIR depuis 2015 reposent sur le couple détection et neutralisation. Notre travail est d'écouter le spectre de radio fréquences, de repérer les protocoles de communication des drones commerciaux et de les traduire visuellement au travers d'un centre de commande et de contrôle (C2) pour faciliter la prise de décision dont la finalité est la *« neutralisation intelligente »* (optimisation de la puissance sur les fréquences utiles, limitation des effets collatéraux en ne brouillant que ce qui est vraiment utile).

ROBOOST : Je parle principalement des drones, donc des robots aériens. Pour rappel le terme drone provient de « faux bourdon » donc ça concerne les objets qui volent. Même si à présent vous êtes nombreux à utiliser le terme drone pour tous les robots. Je parle principalement de notre produit *DroneBlocker* conçu et développé avec notre partenaire *TrustComs*, même si ROBOOST est actif via d'autres produits avec d'autres partenaires.

Notre choix technologique prioritaire est la radiogoniométrie pour la détection et la neutralisation, car dotée d'outils IA et Cyber la détection est très efficace et permet de reconnaitre et d'identifier le drone précisément, la neutralisation est obtenue via la déconnexion (coupure de la liaison de données) voire la prise de contrôle du drone

Cette technologie est très efficace partout y compris en environnement urbain, elle est tout temps H24/7, et enfin et surtout elle permet des neutralisations sélectives : seul le ou les drones cibles sont neutralisés. Bien entendu la capacité est illimité en détection, et en neutralisation le système sait faire face à un essaim de drones.

ROBOOST est intégrateur système, et nous savons pertinemment qu'il n'y a pas de *« silver bullet »* en LAD. Tous les systèmes ont des forces et des faiblesses, donc nous complétons *DroneBlocker* avec d'autres systèmes dans le cadre d'un dôme de protection multi couches, suivant le type de menace à prendre en compte.

MC2 TECHNOLOGIES : Notre PME française basée près de Lille, est spécialisée depuis 2004

dans la conception de composants et de dispositifs hyperfréquences destinés aux applications civiles et militaires. À ce titre, l'entreprise a choisi de mettre à profit son savoir-faire dans le développement d'une gamme complète de solutions (détection & neutralisation) dédiée à la lutte anti-drone.

La technique du brouillage de drones consiste à parasiter les liaisons entre un drone et sa télécommande. Il faut comprendre qu'un drone communique avec sa télécommande (pour échanger les ordres et les données utiles comme la position du drone ou le retour vidéo) sur des bandes de fréquences précises et à des puissances qui sont réglementées par les agences nationales.

Pour brouiller le drone, il faut donc envoyer un signal parasite sur les fréquences concernées. Pour qu'il soit efficace, ce signal doit être plus puissant que celui de la télécommande.

On peut imager cela par une conversation entre deux personnes (le drone et sa télécommande) dont la discussion serait perturbée par une troisième (le brouilleur) qui viendrait crier entre eux.

La distance à laquelle le brouillage sera efficace dépendra aussi des distances entre le drone et son pilote et entre le brouilleur et le drone.

En reprenant notre analogie, il est facile de comprendre que si les 2 personnes qui discutent sont côte à côte, elles seront moins gênées par une personne criant à trois mètres qu'à un mètre d'eux.

Lorsqu'un drone est brouillé, il sera comme « sourd » et restera en stationnaire. Certains sont équipés d'un système de retour à la base (*« return to home »*) leur permettant de rentrer à leur point de départ grâce aux coordonnées GNSS (Géolocalisation et Navigation par un Système de Satellites). Si le brouillage est activé sur la bande de communication GNSS alors le drone sera quand même neutralisé.

Il existe plusieurs bandes de fréquences sur lesquelles communiquent les drones et leurs commandes, mais il existe aussi des communications entre les drones et les satellites GNSS (GPS, Galileo, Beidu, Glonass), pour qu'ils puissent se repérer ou pour qu'ils puissent voler en mode automatique (en survolant des points préprogrammés) ou pour retourner au point de départ (*« return to home »*).Les solutions que nous développons permettent aussi de brouiller ces communications.

Tous les brouilleurs fonctionnent sur ce principe de base. Bien sûr là où MC2 Technologies se différencie c'est dans l'efficacité des signaux de brouillages émis.

En effet, la technologie développée par MC2 Technologies permet de contrer tous les types de protocoles même ceux basés sur des codes de correction d'erreur très performants qui permettent habituellement de corriger la liaison en cas de forte perturbation. Pour des raisons de confidentialité évidentes nous ne pourrons pas fournir d'avantages de détails.

L'autre atout de MC2 Technologies réside dans la sécurité des opérateurs. Qui dit émission

d'ondes électromagnétiques dit potentiel danger sur la santé. Dès leur conception, nous avons pris en compte pour chacun de nos produits, la santé des opérateurs qui utilisent nos matériels. C'est pourquoi nous faisons passer des tests à nos brouilleurs pour vérifier qu'ils ne présentent aucun risque à l'utilisation.

Enfin, en étant à l'écoute des retours d'expériences et des remarques d'opérateurs qui ont l'expérience du terrain, nos équipes de R&D améliorent sans cesse nos produits pour apporter des solutions toujours plus appropriées aux conditions opérationnelles.

Tous ces facteurs font de MC2 Technologies le leader français de la neutralisation de drone.

Notre gamme est très complète :

- **NEROD HG (pour *HandGun* ou pistolet) :** Il s'agit de notre dernière solution de brouillage portable directif ultra-compacte et ultralégère qui se présente sous la forme d'un pistolet ambidextre et monobloc embarquant les modules de brouillage, les antennes et la batterie. Rapidement utilisable et facilement transportable, il a été conçu pour apporter aux forces une protection rapprochée et constitue le dernier rempart face aux attaques de drones. Efficace contre un large spectre de drones, il permet de neutraliser trois bandes de fréquences. Quand toutes ces bandes sont activées, il dispose d'une autonomie confortable d'une heure et demie en fonctionnement. Grâce à son ergonomie et à sa faible masse (2kg en opération) l'utilisateur peut le saisir d'une seule main et l'utiliser comme une arme de poing.
- **NEROD RF (pour « *Rifle* » ou fusil) :** C'est la dernière version de notre fusil brouilleur portable directif développée par MC2 Technologies. Cette version de NEROD a été optimisée à la suite des différents retours d'expérience. Par rapport aux versions précédentes (NEROD F5 notamment), la compacité, l'ergonomie et les performances ont été améliorées. Il s'agit d'un fusil ambidextre et monobloc embarquant les modules de brouillage, les antennes et la batterie. Il s'agit d'une arme polyvalente pouvant être utilisée de manière offensive ou défensive, et de riposter avec aisance à toute attaque de drone. Efficace contre la grande majorité des drones, il couvre les sept bandes de fréquence. Quand toutes ces bandes sont activées, il dispose d'une autonomie confortable d'une heure en fonctionnement.
- **MAJES :** C'est un système de brouillage modulaire permettant d'être utilisés de manière « *fixe* » (pour protéger des sites d'importances) ou de manière « tactique » (protection d'installations temporaires, de véhicule, etc.). Il se compose de plusieurs valises renforcées et étanches contenant les modules de brouillage, l'ordinateur de bord et le système d'alimentation. Ainsi il est très rapidement déployable et facilement transportable. Il fonctionne sur le même principe que les brouilleurs mobiles, mais permet d'émettre des signaux plus puissants et de couvrir une plus grande zone. Il peut être utilisé en configuration « omnidirectionnelle » le brouillage émis forme alors une véritable bulle de protection autour des antennes ; ou en version sectorielle. Dans ce cas, le brouilleur est relié à des plusieurs antennes, dont chacune couvre un secteur à couvrir. L'opérateur pourra alors sélectionner le secteur à activer en fonction de la position de la menace. Ce système permet de limiter les perturbations dans un environnement limité. Cette configuration implique d'être munie d'un système de localisation de la menace. Au

niveau de la couverture, un seul MAJES permet de couvrir de 3 à 6 bandes de fréquence en fonction des besoins, mais nous proposons aussi des solutions sur mesure, permettant de couvrir plus de bandes fréquences selon les besoins Grâce à son aspect modulaire, MAJES peut devenir multi-rôles puisqu'il peut aussi bien couvrir d'autres fréquences de commandes de drones que des fréquences utiles au déclenchement d'IED.

- **FLYJAM :** FlyJam est une solution de brouillage volante efficace contre 95% des drones commerciaux. Né de la collaboration entre les sociétés BP Solutions et MC2 Technologies, FLYJam est l'unique solution du marché qui propose un système de brouillage embarqué. Facile à utiliser et intuitif, il est adapté pour agir au cœur de la menace et en avant de la position de défense. Il garantit ainsi une sécurité maximale du site sous protection en prévenant toute intrusion de drones malveillants FLYJam possède une autonomie de fonctionnement de 1h00 (Vol + brouillage). Ce système est efficace contre les essaims de drone.

MC2 Technologies développe aussi des systèmes de détection ultra performants utilisant l'analyse spectrale en temps réel et une architecture radar 4D fonctionnant dans le domaine térahertz.

TB : Par rapport au choix que vous avez fait, partagez-vous les limites que l'article souligne ?

CERBAIR : Complètement, nos solutions (qu'elles soient mobiles ou sur une embase fixe) a déjà été intégrée à d'autres moyens de détections (radar et optronique). Nous avons conscience que la solution RF peut présenter des limitations dans certains cas (par de liaisons RF ou bien fréquences utilisées n'ont pas pu être déterminées). Toutefois, notre analyse du marché nous amène à penser que la grande majorité des drones continuera à utiliser des liaisons RF que ce soit pour des nécessités de prise de vue (espionnage ou propagande) et/ou d'attaque afin de cibler correctement l'objectif.

ROBOOST : En détection la radiogoniométrie associée à de l'IA et de la Cyber permet de pallier les faiblesses que vous citez. Et contrairement à d'autres systèmes de neutralisation, une localisation très précise n'est absolument pas nécessaire pour réussir la neutralisation. En neutralisation, la radiogoniométrie associée à de l'IA et de la Cyber permet de neutraliser tous les drones y compris avec des liaisons cryptées, obtenue par déconnexion/coupure de la *datlink*. L'identification est parfaite, d'une part le système donne le modèle de drone mais en plus son N° Mac, tout comme pour la télécommande. Mais effectivement cela nécessite une base de données. De plus nous avons la capacité à hacker la vidéo du drone : ceci permet d'améliorer l'évaluation et la classification de la menace.

MC2 TECHNOLOGIES : Nos systèmes permettent de brouiller les liaisons radio-fréquences et les moyens de navigation par GNSS, ils permettent donc de neutraliser la quasi-majorité des drones. Contrairement à ce que vous évoquiez, il n'est pas toujours nécessaire d'identifier la ou les fréquences utilisées. Dans 98% des cas, les drones utilisent des bandes de fréquences standards. Pour neutraliser ces drones et

avoir une très grande probabilité de succès, il suffit donc de couvrir un maximum de ces bandes de fréquences, c'est ce que permettent nos systèmes.

L'identification des bandes utilisées a un intérêt lorsque l'on veut limiter l'impact du brouillage sur l'environnement, et éviter de perturber toutes les installations environnantes en ne brouillant que les bandes nécessaires. Cela peut être réalisé en couplant les brouilleurs à des systèmes d'écoute radio-fréquence par exemple.

D'autre part, vous soulignez à juste titre, qu'aucun moyen de lutte anti-drone n'apporte de solution « miracle ». Cependant, il est possible de les allier pour les renforcer. Par exemple, un drone présentant une menace sera stoppé grâce à un brouilleur. Pendant que celui-ci est bloqué, un périmètre de sécurité pourra être établi pour qu'un tireur puisse le détruire.

TB : Comment abordez-vous la problématique de l'identification des drones par rapport aux oiseaux et les risques liés au bio-mimétisme ?

CERBAIR : L'avantage de la solution RF est qu'elle est indépendante de la cinématique ou de la forme de l'objet. Un oiseau n'a pas de télécommandes et un drone biomimétique en a besoin. L'avantage de la solution RF est que cette question ne se pose pas à notre niveau.

ROBOOST : La radiogoniométrie n'est absolument pas impactée par cette problématique.

MC2 TECHNOLOGIES : Ce genre de problématique peut être abordée en couplant les moyens de détection, par exemple en associant un radar, avec un ou des système(s) d'écoute RF, et des caméras à haute résolution et en centralisant les informations. De notre côté, nous avons fait le choix d'une technologie de radar très haute résolution offrant une capacité d'identification inégalée couplée à une solution d'analyse spectrale en temps réel intelligente.

TB : Comment l'arrivée de la 5G, la navigation autonome ou les drones en essaims peuvent impacter votre solution ? Sont-ils foncièrement si différents à détecter qu'un drone du commerce ? Quelles réponses mettez-vous en place pour y répondre ?

CERBAIR : Ce sont trois problématiques différentes.

- D'abord, concernant la 5G, cela posera un problème. C'est certain. Mais pas différent de celui posé par des drones pilotés en 4G. La difficulté repose sur l'extraction dans les flux GSM de ceux impliquant un drone. C'est très difficile, nous n'avons pas encore la réponse mais c'est une question sur laquelle nos ingénieurs en RF et en guerre électronique travaillent d'arrache-pied. Nous pensons aussi que dans un certain nombre de cas, le

pilotage par GSM n'est pas forcément possible car il nécessite une infrastructure fixe. Cela impose que les drones soient en portée du réseau GSM. Si cela ne pose pas trop de problème dans les villes des pays occidentaux, il en est tout autrement dans les campagnes ou les lieux désertiques. Ce moyen de pilotage n'est pas adapté partout. En plus, les restrictions de vol des drones, suite aux réglementations, font qu'il est assez difficile de faire voler un drone en ville ou en zone péri-urbaine. Par conséquent, le réseau GSM n'est peut-être pas, aujourd'hui, le moyen le plus pertinent pour piloter un drone. L'avenir nous dira ce qu'il en est.

- D'autre part, concernant les drones autonomes, il nous faut nous interfacer avec un autre moyen de détection (radar) mais aussi réfléchir à d'autres moyens de neutralisation car le brouillage n'est alors plus pertinent. C'est un cas que nous prenons au sérieux mais toutefois nous restons convaincus qu'il s'agit d'un scenario marginal pour le simple fait qu'il maintenir une liaison radiofréquences.
- Enfin, notre solution détectant les liaisons RF, peu importe le nombre de drone en vol. C'est un cas d'autant plus intéressant que le vol en essaim impliquera très probablement des liaisons RF que ce soit entre le ou les pilotes ou entre les drones en eux-mêmes afin de garder leur coordination. C'est un cas ou notre solution s'avère très pertinente que ce soit pour la détection ou la neutralisation par brouillage.

ROBOOST : Ces nouvelles menaces sont prises en compte, le vol en essaim est opérationnel. En radiogoniométrie oui, il faut couvrir la 5G et si autonome signifie sans liaison de données il faut y associer une autre technologie de détection. Nous avons lancé un programme de R&D, et ciblé des partenaires apportant la ou les briques technologiques complémentaires.

MC2 TECHNOLOGIES : Les solutions développées par MC2 permettent de détecter et neutraliser ces menaces mais pour des raisons de confidentialité nous préférons éviter d'étayer d'avantages la présentation de nos solutions.

TB : La menace potentielle représentées par des drones terrestres et maritime fait-elle aussi partie des menaces que vous prenez en compte ?

CERBAIR : Oui, même s'il n'y a pas encore de demande par rapport ces drones. La problématique reste la même, surtout pour les drones terrestres qui sont, au niveau de leur architecture de télécommande très proche voir identique à celle des drones aériens. Nous n'avons pas encore été confrontés à des drones maritimes mais notre approche sera la même.

ROBOOST : Oui, mais en second plan à ce jour.

MC2 TECHNOLOGIES : Oui, nos systèmes sont conçus pour neutraliser tous les types de protocoles de communication sans fil entre un pilote et son drone, qu'il soit aérien, terrestre ou maritime.

TB : Voici quelques semaines le sénateur républicain de l'UTAH, Mike Lee, a publiquement demandé que des sociétés de sécurité privées aient le droit de brouiller des drones malveillants. Quel est votre sentiment sur cette position ?

CERBAIR : Cela peut être intéressant que certaines sociétés privées soient habilitées car les services étatiques (police, justice, douanes, gendarmerie, armée) ne peuvent pas tout assumer. Mais cela risque d'être un processus très long et compliqué juridiquement.

ROBOOST : C'est un sujet que nous avons traité lors de notre projet SPID, retenu par le SGDSN en 2015. Cette mission d'intervenir sur des aéronefs et engins en vol est de la responsabilité du CDAOA. Mais compte tenu de l'ampleur du sujet, cette mission a été déléguée à certains ministères (Intérieur avec la Gendarmerie et la Police, Justice avec l'Administration pénitentiaire, et ça va se poursuivre avec d'autres ministères) mais comme la sécurité de nombreux sites civils et également militaires est de plus en plus confiée à des sociétés privées, il est clair qu'un jour les agents de sécurité privée auront cette capacité, dans un cadre règlementé.

MC2 TECHNOLOGIES : En France, le brouillage ne peut être réalisé que par les forces de l'ordre. En effet, l'article L33-3-1 du code des postes et des communications électroniques prohibe l'installation, la détention et l'utilisation de tout dispositif destiné à rendre inopérants des appareils de communications électroniques de tous types, tant pour l'émission que pour la réception. Le non-respect de cette interdiction est sanctionné de 6 mois d'emprisonnement et 30 000 euros d'amende (article L39-1 du Code des postes et communications électroniques).

L'utilisation des brouilleurs de drones par des sociétés privées est une décision politique. En tant qu'industriel, il est difficile de nous positionner. Cependant, nous constatons que les entreprises privées sont de plus en plus confrontées à la *« menace drone »* : Survol de site intempestif, espionnage… Ces sociétés cherchent à de doter d'équipements performants mais leurs choix est très limité.

Dans le cadre du continuum de sécurité, le dernier livre blanc sur la sécurité intérieure cherche à étendre les compétences et prérogatives de la sécurité privée. L'objectif est d'accorder de nouvelles compétences à la sécurité privée et notamment, l'usage des nouvelles technologies. Ces technologies comprennent la lutte anti-drone. Nous assistons donc à une évolution des mentalités sur ce point. L'utilisation des systèmes est peut-être en cours d'évolution au profit des sociétés de sécurité privées.

TB : Peut-on craindre des dérives dans les années à venir sur le brouillage, un acte qui est considéré par beaucoup comme un acte de

guerre ?

CERBAIR : Pas forcément, si le matériel dédié à cet usage est juridiquement correctement encadré sur ses performances que ce soit pour la puissance émise et les bandes de fréquences concernées.

ROBOOST : Les systèmes de brouillage sont en France assimilés à des matériels de guerre. Les utiliser en international est effectivement considéré comme acte de guerre et cela va perdurer. Un groupe de travail international travaille sur la LAD, leur objectif est de classer à terme tous les moyens de détection et de neutralisation des drones.

MC2 TECHNOLOGIES : Les brouilleurs de drones sont classés matériels de guerre. Leurs fabrications et leurs utilisations sont très encadrés par l' État. Les dispositifs mis en place permettent de limiter considérablement les éventuelles dérives.

TB : Aujourd'hui qu'elles sont les réponses possibles juridiquement accessibles à un acteur privé pour contrer un drone ?

CERBAIR : C'est effectivement un problème. Aujourd'hui beaucoup d'acteurs privés hésitent à s'équiper en équipement anti-drone faute de solution de neutralisation adaptés. S'ils peuvent détecter la menace, ils restent impuissants pour la neutraliser. Tout juste peuvent-ils dépêcher leur équipe de sécurité sur le point ou se situe le pilote. C'est un point que l'article décrit très bien. Cette problématique est un axe de réflexion majeur chez CERBAIR.

ROBOOST : Il faut être associé à un représentant étatique parmi ceux cités plus haut pour obtenir son GO quant à une neutralisation.

MC2 TECHNOLOGIES : Aujourd'hui, les réponses juridiques sont très limitées. La solution la plus pertinente est la mise en place de *No Fly Zone*. Ces zones sont mises en place en collaborations avec les fabricants de drones. Malheureusement, ces *No Fly Zones* peuvent être contournées. L'autre réponse consiste à contacter les forces de l'ordre qui prendront le cas échéant des mesures, mais le délai d'intervention est pour le moment trop long.

Nous remercions vivement CERBAIR, ROBOOST et MC2 TECHNOLOGIES d'avoir aimablement répondu à nos questions.