FACE AU RISQUE
LA RÉFÉRENCE DES ACTEURS DE LA MAÎTRISE DES RISQUES
Pays : FR
Périodicité : Mensuel

Date : Decembre 2019
Page de l'article : p.46-47
Journaliste : Séverine Fontaine

Économie et technologies

Quel type de drone ? A-t-il des intentions menaçantes ? » Des technologies de détection permettent également de réaliser cette tâche comme le radar passif, la goniométrie, l'écoute des messages caractéristiques des drones ou encore l'acoustique.

Le système doit également suivre l'évolution de la menace dans le temps et comprendre l'intention du drone. « *Pour cela, on travaille sur des systèmes à base d'intelligence artificielle, notamment l'apprentissage profond, capables d'exploiter le maximum d'informations contextuelles pour une compréhension la plus fine possible. L'un des enjeux est d'être capable de fusionner les données et exploiter le mieux possible la complémentarité des technologies pour avoir l'information la plus pertinente.* »

La dernière étape sera de neutraliser pour stopper la menace, sujet central du séminaire international dédié à la lutte anti-drones.

> **Les entreprises doivent reporter les incidents, déposer une plainte et, en interne, donner des instructions aux opérateurs.**
>
> **Colonel Jean-François Morel,** Direction générale de la Gendarmerie nationale.

Des démonstrations de neutralisation. Ainsi, les 16 et 17 octobre 2019, des entreprises spécialisées dans ces technologies se sont regroupées à l'aéroport d'Avignon pour une journée de démonstrations. Ces dernières se sont déroulées dans un contexte bien précis, comme nous l'explique Hubert Bérenger, responsable des programmes Drones et Aéronefs légers chez Safe Cluster, l'organisateur de la manifestation : « *Nous avons été missionnés par le Gouvernement pour trouver des technologies de neutralisation de drones dans le cadre des Jeux olympiques d'été 2024 qui se dérouleront en France. Nous avons cherché dans notre réseau quelles entreprises pourraient répondre à la demande. Dans les vingt-trois repérées, nous en avons sélectionné sept.* » Six d'entre elles – Thales Six, Thales Las, CS, Roboost, UrWings/MC2 et Cerbair – ont réalisé quatorze démonstrations allant du brouillage de communication à la maîtrise physique du drone.

L'industriel CS Group a par exemple fait la démonstration de différentes séquences de brouillage électromagnétique. Le brouillage directif piloté par le poste de commande et de contrôle de leur système Doreades permet de concentrer la neutralisation sur la cible limitant ainsi les impacts sur l'environnement, et le brouillage omnidirectionnel formant une « bulle de protection » autour du site pour empêcher les attaques d'essaims de drones venant de plusieurs directions.

Une autre démonstration a été réalisée avec un drone intercepteur. La société travaille actuellement sur la mise en œuvre d'un brouilleur de faible puissance embarqué sur le drone intercepteur pour forcer l'atterrissage du dispositif chassé tout en limitant son impact électromagnétique par sa proximité avec la cible.

La société Cerbair a quant à elle présenté son dernier produit, le « Manpack ». Il s'agit d'une solution tout-en-un de détection par analyse radiofréquence passive, de caractérisation et de neutralisation des drones dans un système portable – un sac à dos – pour un individu. « *Notre solution permet une détection dans un rayon de 1,5 km,* explique Philippe Rouin, vice-président marketing de la société. *Lors de la détection, l'opérateur reçoit une notification via une tablette tactile ou un signal audio. Il utilise l'antenne pistolet pour affiner la détection et peut, par pression d'un simple bouton, forcer l'atterrissage du drone malveillant.* »

Roboost, filiale de Byblos Group, a présenté une solution de radiofréquence avec prise de contrôle du drone. L'entreprise a étendu son savoir-faire dans la prise de contrôle des aéronefs wifi aux technologies s'appuyant sur des communications radiofréquence non wifi. « *Nous savons cibler et poursuivre les fréquences de manière très rapide, avec pour certains drones des sauts toutes les 2 millisecondes et un changement de bande de fréquences* » affirme Romaric Foucard, responsable de programme chez Roboost.

L'industriel Thales propose de son côté trois solutions de neutralisation : le détournement de drone par prise de contrôle de son système de guidage, le brouillage en saturant les bandes de fréquences spécifiques et des zones radio, et l'interception des drones – en essaim par exemple – par le déploiement de filets ou ondes électromagnétiques. « *Ce drone, plus musclé, vole à 150 km/h en allant à la rencontre des drones intrus pour envoyer un filet par air comprimé* », détaille Philippe Rouin de Cerbair, présent lors des démonstrations. Ce qui nécessite un opérateur disponible 24 h sur 24. Et c'est là que le bât blesse…

Faire évoluer la réglementation. Aujourd'hui, beaucoup de technologies sont développées, mais le cadre juridique ne permet pas leur pleine exploitation. En effet, l'achat et l'utilisation des technologies de neutralisation ne sont autorisés en France, par dérogation, qu'aux besoins de l'ordre public, de la défense et de la sécurité nationale, ou du service public de la justice, comme le décrit l'article L.33-3-1 du code des postes et des communications électroniques (CPCE). « *Les technologies de brouillage sont des armes de guerre dont l'usage est limité par la réglementation,* confirme le colonel Jean-François Morel de la Gendarmerie nationale. *Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) demande aux entreprises de développer des technologies nouvelles car il y a un besoin opérationnel. Il faut en parallèle faire évoluer le droit. Quand un drone est détecté sur un site, on ne peut pas appeler le 17 pour demander une intervention. La menace drone est trop rapide. Nous avons besoin d'autres acteurs formés pour s'en occuper.* » De plus, certaines technologies de brouillage sont encadrées puisqu'elles peuvent avoir un impact sur les équipements qui reposent sur ces systèmes. C'est le cas notamment du GPS par les avions.

Formation de militaires. En attendant l'évolution de la réglementation, près de trois cents opérateurs gendarmes sont aujourd'hui formés et déployés sur le territoire français pour protéger ponctuellement certains sites, comme les sites Seveso, les événements publics, comme par exemple la braderie de Lille, ou répondre à des problématiques spécifiques (le Puy du Fou, les centres d'essais automobiles) mais aussi des aéroports avec la gendarmerie des transports aériens. En plus de ces

Tous droits réservés à l'éditeur

FACE AU RISQUE
LA RÉFÉRENCE DES ACTEURS DE LA MAÎTRISE DES RISQUES
Pays : FR
Périodicité : Mensuel

Date : Decembre 2019
Page de l'article : p.46-47
Journaliste : Séverine Fontaine

opérateurs à temps plein, répartis dans les sept zones de défense en France, on compte vingt-et-un militaires formés et exécutant cette mission à temps plein au sein de la Garde Républicaine à Paris, qui protègent notamment les Palais nationaux mais pouvant être appelés ponctuellement en renfort sur des opérations de province ou d'outre-mer.

Des obligations pour les utilisateurs de drones civils. La loi « drone » n° 1428-2016 du 24 octobre 2016 impose sept obligations aux utilisateurs de drones civils de plus de 800 grammes, comme l'enregistrement, la formation des télépilotes, ou encore le signalement électronique et lumineux. Celle-ci se traduit par la mise en place d'un système d'information étatique (SIE) permettant l'identification de ces drones via une plaque d'immatriculation. Celle-ci serait soit intégrée dès la construction du drone, soit ajoutée par puce sur les plus anciens. Il permettra par exemple d'identifier les drones en infraction, d'identifier le niveau de menace et d'aider à la décision.

Former les responsables sécurité. Les responsables de sécurité considèrent de plus en plus la menace drone. Il y a quelques années, la perception du drone civil se rapportait plus au jouet. Aujourd'hui l'actualité prouve que le drone peut être une arme. « *Nous devons encore expliquer les capacités des drones – ce qu'ils sont capables de faire – mais également l'état de l'art de la lutte anti-drones* » ajoute le représentant de Cerbair. Tous n'y sont pas sensibilisés ou formés. La Gendarmerie nationale a par exemple réalisé des interventions auprès des opérateurs de sites Seveso pour les éveiller aux problématiques drones, « *mais cela reste compliqué car ils n'ont ni les outils, ni la possibilité d'y faire face réellement* », explique le colonel Jean-François Morel.

Leurs seules possibilités sont les technologies de détection (visuelle, comme un simple drone caméra, ou radiofréquence), le signalement ou encore la plainte. « *Les entreprises doivent reporter les incidents, déposer une plainte et, en interne, donner des instructions aux opérateurs. Que doivent-ils faire s'ils voient ou trouvent un drone ? Ne pas le toucher ou le déplacer ?* ». Mais ces entreprises doivent également comprendre en quoi elles sont vulnérables, en quoi un drone peut représenter une menace, donner des fiches réflexe aux agents de sécurité ou encore savoir s'il y a des points de décollage à proximité du site.

Il est également important de rappeler que la plupart des technologies utilisées en France sont des drones de loisirs – vendus par milliers chaque année – que l'on peut acquérir pour quelques milliers d'euros, pour les plus performants. Alors que les technologies développées en face sont bien plus coûteuses, quelques dizaines de milliers d'euros, en fonction de leurs capacités. Un affrontement inégal en termes de technologies et de coûts.

Même si l'ensemble des technologies de lutte anti-drones ne sont pas accessibles aux responsables sécurité, la « menace drone » doit nécessairement être intégrée dans leur politique de sécurité.

Séverine Fontaine

Le système portable anti-drones permet à l'opérateur de détecter un dispositif dans un rayon de 1,5 km et de le neutraliser.

Tous droits réservés à l'éditeur