Drones civils : réponses opérationnelles et juridiques aux usages malveillants

La protection contre le large spectre d'utilisation malveillante de drones aériens nécessite des solutions techniques pour leurs détection, identification et neutralisation. L'arsenal juridique doit être renforcé en matière de responsabilisation et de sanctions.

Ces aspects de la prolifération des drones civils ont été abordés au cours d'un colloque organisé, le 28 mai 2015 à Paris, par le Secrétariat général de la défense et de la sécurité nationale et le Conseil économique, social et environnemental. Y sont notamment intervenus : le contre-amiral Frédéric Renaudeau, directeur de la protection des installations, moyens et activités de la défense au ministère de la Défense ; Patrick Espagnol, directeur de la sécurité d'EDF ; Thierry Michal, directeur technique général de l'Office national d'études et de recherches aérospatiales (ONERA) ; Thomas Andrieu, directeur des libertés publiques et des

affaires juridiques au ministère de l'Intérieur ; Bruno Delor, président de la Fédération française d'aéromodélisme.

Adaptation du dispositif de défense. Il s'agit d'abord d'évaluer les besoins de protection, à savoir les installations sensibles, événements particuliers (rencontres politiques, musicales ou sportives), populations et personnalités dans des environnements parfois complexes. Selon l'amiral Renaudeau, un drone distant de 6.000 m et volant à 70 km/h est détecté avec 5 minutes de préavis, dont 1 minute pour la prise de décision. La radiogoniométrie seule ne suffit pas pour interpeller un téléopérateur malveillant, en raison de la diversité des modes de pilotage. Elle est complétée par le radar et les détections acoustique et optronique (équipement combinant l'optique et l'électronique). L'identification, principe de base de la sécurité aérienne, est essentielle pour éviter les méprises : vol licite ou non, objet volant ou oiseau. Le sentiment d'impunité se combat ainsi depuis le sol par les moyens optroniques. Les accords avec les grands opérateurs de téléphonie mobile permettent d'obtenir un signalement du drone, du « télépilote » ou de l'intention de survol. La neutralisation porte d'abord sur la protection passive par des systèmes aériens, aquatiques ou terrestres, simples et intégrés aux autres fonctions d'autoprotection des sites. Ensuite, elle consiste à brouiller ou leurrer le système de navigation du drone sans le détruire. Enfin, la destruction du drone s'effectue par tir d'arme de précision ou d'un fusil de chasse à chevrotine, selon un cadre juridique de l'emploi de la force après analyse des risques et dommages collatéraux possibles. Une autre solution implique la capture du « microdrone » malveillant au moyen d'un filet transporté par un drone intercepteur. Le commandement et le contrôle des actions de neutralisation reste en cohérence avec la défense aérienne, qui centralise les informations. Le ministère de la Défense élabore des plans d'équipement des sites sensibles, en fonction des vulnérabilités et réponses technologiques disponibles. Mais, souligne l'amiral, le cadre juridique doit évoluer en priorité en matière de neutralisation/destruction et de signalement des drones.

Filière industrielle de la sécurité. Soucieux de protéger son patrimoine, EDF doit assumer ses responsabilités de sécurisation de la population et de l'environnement, dont les centrales nucléaires, rappelle Patrick Espagnol. Il doit donc anticiper cette nouvelle menace complexe et sophistiquée avec surmultiplication des cibles par l'interconnexion. Chaque famille de drones suit sa logique propre, qu'il convient de détecter par expérimentation. Puis, il faut

maîtriser le drone malveillant en l'obligeant à se poser à un endroit déterminé. Opérateur privé avec obligation de résultat, EDF compte sur l'État, client et fournisseur de sécurité, pour une mise en commun des réflexions et expertises dans ce domaine. La Gendarmerie et l'armée de l'Air sont chargées de faire respecter l'interdiction de survol de sites sensibles. En matière de sécurité, la réponse doit être adaptée, sans coût excessif, supranationale et s'appuyer sur l'existant, la recherche et le développement, selon Patrick Espagnol.

Vaste domaine de recherche. L'ONERA, explique Thierry Michal, présente un aspect dual. Acteur de la recherche aéronautique, il doit remplir des missions de plus en plus exigeantes dans le respect des règlements. Parallèlement, avec son volet défense, il doit lutter contre tout usage malveillant dans ce domaine. Le contenu très sophistiqué de la charge utile du drone correspond à des besoins variables. Dans ce contexte, il s'agit de mettre en place un système pour contrer la menace future. La détection restera complexe, compte tenu de l'évolution rapide de la technologie des drones. Par ailleurs, la réponse sera globale avec la mise en œuvre d'une chaîne de mesures reposant sur le dynamisme de la filière robotique. Compte tenu de la prolifération des drones bon marché et aux discrétion et capacité d'action accrues, il faudra des capteurs compacts et des senseurs performants. Ceux-ci devront être autonomes en matière de durée d'intervention et de furtivité, à savoir peu détectables ou identifiables. Les drones civils sont en effet particulièrement furtifs, car construits sans métal et volant à très basse altitude dans un environnement urbain. La lutte anti-drones va privilégier la rapidité et « l'approche système », à savoir détection, identification, décision et neutralisation, cohérence essentielle de la chaîne de défense. La tendance s'oriente vers une solution la plus automatisée possible. Mais, prévient Thierry Michal, il faut réfléchir à la place de l'homme dans la boucle, domaine de recherche de l'ONERA.

Difficultés juridiques. Il n'est pas toujours possible d'identifier la provenance des drones et de les arrêter, indique Thomas Andrieu. Par ailleurs, la lutte contre leur usage malveillant ne doit pas conduire à brider un domaine économique en plein essor, au nom de la liberté du commerce et de l'industrie ainsi que du développement de ce secteur. Les critères retenus portent sur le poids et la taille du drone. Les conséquences dommageables posent la question de l'assurance, pas encore disponible. La destruction à distance n'est autorisée que si la menace est identifiable et prouvable. La réglementation prévoit des obligations : information

sur les conditions d’utilisation ; formation minimale ; enregistrement et signalement électronique. Il faut ensuite faire le tri entre les types de drones et les malveillances potentielles. Au niveau de l’Union européenne, certains États exigent la présence d’une puce d’identification électronique.

Loïc Salmon

Drones civils : avantages, mais aussi sources de menaces complexes et évolutives

Les drones Un peu d’histoire

La Fédération française d’aéromodélisme regroupe 850 associations totalisant 28.000 licenciés. Pour limiter le risque d’utilisation malveillante des drones de loisir, elle recommande notamment : la mise en place d’un site internet officiel de sensibilisation ; l’incitation des fabricants et vendeurs à une information pour une utilisation licite ; le renforcement du principe de déclaration des sites de vol en groupe ; l’identification électronique et un brevet de « télépilote » pour les drones au dessus d’un seuil de masse à définir.