

rapport de 2012 de la Cour des comptes américaine, «Aucune technologie déployée ne confère [aux aéronefs sans pilote] la capacité de détecter et d'éviter les aéronefs et les autres objets dans les airs» tout en satisfaisant aux réglementations aériennes.

Éviter les autres appareils est particulièrement difficile pour les petits drones, car ils ne peuvent pas embarquer les systèmes de radar existants, trop encombrants et gourmands en électricité. Les caméras en lumière visible et infrarouge offrent une alternative efficace, mais elles ne voient pas à travers les nuages.

À terme, une solution pourrait venir de l'ADS-B (*Automatic Dependent Surveillance-Broadcast*), un système développé à partir des années 1990. Il se fonde sur des «transpondeurs» embarqués, qui signalent toutes les secondes la position et la vitesse de l'appareil, et reçoivent des informations

équivalentes des aéronefs évoluant dans la même zone. D'ici 2020, tous les appareils volant dans l'espace aérien américain, petits ou gros, avec ou sans pilote, devront être équipés de transpondeurs ADS-B. Ainsi, les collisions pourront être évitées.

Comme le GPS civil, l'ADS-B a un talon d'Achille: ses émissions ne sont pas authentifiées et peuvent donc être contrefaites. Au début de son développement, la sécurité était une préoccupation mineure, car personne n'imaginait que l'on puisse diffuser de faux signaux. Aujourd'hui, il est facile et peu coûteux de leurrer ce système. En 2012, des chercheurs de l'Institut de technologie de l'Armée de l'air américaine, dans l'Ohio, ont montré que des attaques variées, fondées sur de faux signaux, peuvent être lancées depuis le sol ou les airs avec une antenne bon marché. De telles attaques, dites de «fausse injection», feraient par exemple

croire à un appareil qu'une collision est imminente.

On peut ainsi émettre des centaines de faux signaux ou empêcher la réception de messages légitimes. De faux signaux ADS-B seraient plus problématiques pour les petits drones que pour un avion doté d'un pilote embarqué. En effet, grâce au radar de bord, un pilote peut rapidement vérifier si la trajectoire de son appareil entraîne un risque de collision.

Une solution envisagée pour authentifier les sources des émissions est la multilatération, une technique consistant à localiser ces sources en mesurant les instants relatifs d'arrivée des signaux sur des récepteurs au sol, puis à relayer cette information jusqu'aux avions en vol. Mais cela suppose de mettre en place un système de géolocalisation différent du GPS (avec des récepteurs au sol au lieu de satellites

Les drones en Europe

Les États-Unis et Israël sont en avance en matière de drones militaires, grâce à leur retour d'expérience en opérations ou lors d'entraînements. Un marché s'y est développé dans les années 1990. L'Europe a utilisé beaucoup moins de drones de ce type (seuls quelques-uns ont servi à des observations au Kosovo, en Iraq et en Afghanistan) et son industrie aéronautique n'a pas bénéficié du marché militaire.

Cependant, les performances européennes sont comparables à celles des États-Unis et d'Israël dans le domaine des drones civils, pour lesquels les priorités sont différentes. Du côté militaire, l'efficacité prime, tandis que le risque d'accident est un paramètre essentiel dans les espaces aériens civils.

On sait aujourd'hui proposer des solutions individuelles à chaque problème identifié : perte de signal GPS pendant quelques minutes, perte de communications, risque de collision, pannes simples, etc. Mais les vols réels impliquent souvent de multiples combinaisons et enchaînements de ces éléments simples, face auxquels les systèmes actuels peinent à remplacer la réactivité de pilotes entraînés et présents à

bord. Il faut alors développer un système global et sécurisé de supervision du vol, où pourraient être programmés les paramètres propres à chaque mission et qui gèrerait les aléas et les défaillances.

C'est le sens des recherches menées par le réseau *Micro Air Vehicle Research Center* (Centre de recherche sur les micro-drones), à Toulouse, coordonné par l'Institut supérieur de l'aéronautique et de l'espace (ISAE) et regroupant un certain nombre d'autres organismes (ENAC, Onera, LAAS-CNRS, etc.). Y sont développés des systèmes de navigation combinant les données du GPS, d'accéléromètres, de caméras, de cartes, de détecteurs d'obstacle, de localisation relative, etc. De tels systèmes devraient

pouvoir détecter les incohérences entre les données introduites par les piratages décrits dans cet article. Diverses applications sont visées, telle l'inspection de grottes archéologiques ou le recueil de données météorologiques.

En attendant l'arrivée de ces systèmes sur le marché, les usages autorisés doivent être restreints, afin de simplifier les problèmes de sécurité rencontrés. En France, une réglementation pour les drones civils a été publiée en 2012. Elle interdit par exemple le survol des zones peuplées sans dépôt d'un dossier de sécurité – un lycéen a d'ailleurs été poursuivi par la justice en février 2014 pour avoir filmé la ville de Nancy avec un drone sans autorisation. Les usages permis se répartissent en quatre scénarios et doivent faire l'objet d'une demande d'autorisation spécifique. L'un de ces scénarios, par exemple, décrit le survol de zones inhabitées, à moins de 50 mètres du sol, dans un rayon d'un kilomètre et hors de la vue de l'opérateur; il

concerne typiquement des applications agricoles.

Pour améliorer la fiabilité des drones, on devra aussi adapter la formation des opérateurs qui les dirigent. Ces appareils ont introduit une nouvelle façon de piloter, qui modifie en profondeur le partage des tâches entre hommes et systèmes, et donc le partage de responsabilité entre pilotes et concepteurs.

Ainsi, la technologie et la réglementation doivent évoluer de concert pour définir des applications des drones adaptées à leurs caractéristiques propres. Malgré leur manque de fiabilité, ces appareils ont de nombreux atouts : gamme de tailles variée, émissions sonores réduites pour les petits drones, pas de mise en danger de la vie des pilotes... Plus que leur coût (le retour d'expérience sur les drones militaires a montré que le coût d'exploitation reste élevé malgré l'absence de pilote à bord), ce sont ces atouts qui favoriseront leur déploiement.

– Patrick Fabiani
Directeur adjoint de la recherche,
ISAE (SupAero & Ensica)

émetteurs), aussi fiable et précis que lui, système dont le coût reste à déterminer.

Enfin, la liaison radio dite de commandement et de contrôle, entre l'opérateur et l'appareil, qui permet de piloter ce dernier, semble *a priori* moins problématique pour la sécurité que le GPS ou l'ADS-B. Des protocoles de communication sécurisés sont définis pour ces signaux, ce qui devrait les protéger des falsifications.

Cependant, les signaux peuvent tout de même être bloqués, d'où une perte de contrôle du drone. Une telle perte de liaison peut résulter d'un brouillage ou d'une autre forme de malveillance. Aucune solution satisfaisante n'a encore émergé. En général, les opérateurs configurent leurs drones avec un protocole de perte de liaison, qui déclenche par exemple le retour vers la base si la liaison radio est perdue pendant plus de 30 secondes. Mais un tel protocole suppose que le système de navigation du drone (lui-même cible potentielle de piratage) fonctionne et que l'appareil n'ait pas été victime d'un problème logiciel, à l'instar de l'hélicoptère Fire Scout ayant approché Washington en 2010.

Une autre difficulté consiste à identifier des régions du spectre radio susceptibles d'être dédiées à la transmission des signaux de commandement et de contrôle. Sans cela, de nombreux drones devront émettre dans des bandes radio non protégées, utilisées pour d'autres types de transmissions. Des interférences involontaires risquent alors de se produire avec les signaux émis par les multiples systèmes électroniques qui occupent déjà ces bandes.

Outre cette complexité technique, la sécurisation de l'espace aérien pour les drones se heurte aux lenteurs bureaucratiques et à l'hostilité des législateurs. Un changement fondamental de la façon de piloter doit être pris en compte. L'opérateur de drone, basé au sol, n'a plus les mains sur le manche et les yeux rivés sur le pare-brise du cockpit. Il entre un itinéraire dans un ordinateur, contrôle le drone avec un dispositif de type joystick et surveille une série de liaisons sans fil grâce auxquelles l'appareil communique avec sa base. Le drone peut alterner des moments où il est piloté comme un jouet télécommandé – mais un jouet pesant parfois plusieurs tonnes ! – et des phases où il vole de façon autonome.

Il faudra développer un système de régulation adéquat du trafic aérien, afin que les drones partagent le ciel en toute

sécurité avec les autres aéronefs, petits et gros. En particulier, il faudra garantir qu'ils ne deviennent pas un danger en cas de perte de liaison.

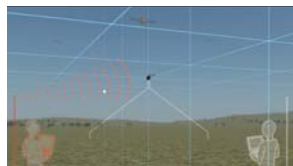
Pour l'Administration américaine de l'aviation, cette mission s'ajoute au développement d'un nouveau système de gestion du trafic aérien, le NextGen (*Next Generation Air Transportation System*). Les nouvelles réglementations devront instaurer un équilibre délicat entre les considérations de sécurité publique et les avantages économiques des drones. En imposant aux aéronefs sans pilote de rester dans la ligne de vision d'un opérateur, on empêcherait sans doute leur détournement, mais on les rendrait inutilisables pour de nombreuses tâches. Les drones soulèvent aussi des questions relatives au respect de la vie privée, et des voix s'élèvent pour demander un encadrement sévère de ces engins capables de survoler un jardin de banlieue avec des caméras haute définition.

Les drones, objets de méfiance

De nombreux législateurs voient d'un mauvais œil l'arrivée des drones, qu'ils ont découverts *via* leur rôle dans des conflits armés. Au moins 42 États américains ont mis en place des lois limitant leur utilisation. Ainsi, au Texas, un drone ne peut filmer une propriété privée sans le consentement du propriétaire – c'est aussi le cas en France, où la CNIL (Commission nationale de l'informatique et des libertés) régit l'usage d'images et d'informations acquises par des drones. Au niveau fédéral, le *Preserving American Privacy Act*, une loi de préservation de la vie privée proposée en 2013, rendrait nécessaire l'obtention d'un mandat pour effectuer une surveillance avec des drones, et illégale l'utilisation de drones armés au-dessus des États-Unis.

Les difficultés techniques et les inquiétudes exprimées par les législateurs devraient ralentir l'adoption des drones, sans toutefois l'arrêter. La sécurité de ces appareils doit être considérée avec un certain recul. Les avions classiques sont aussi vulnérables : ils peuvent être détournés, les pilotes forcés à agir sous la contrainte, les communications coupées. Et pourtant nous continuons à voler, non par ignorance des risques, mais parce que les avantages l'emportent. Les bénéfices des drones nous pousseront aux mêmes concessions. ■

■ EN VIDÉO



Vidéo montrant le piratage d'un drone : <http://tinyurl.com/nwa5atf>

■ SUR LE WEB

Autorisations nécessaires pour faire voler un drone en France : www.developpement-durable.gouv.fr/Demarches-pour-effectuer-le.html

Site de l'ISAE : www.isae.fr

■ BIBLIOGRAPHIE

Les drones aériens : passé, présent et avenir, Documentation française, 2013.

Unmanned aircraft systems : Measuring progress and addressing potential privacy concerns would facilitate integration into the national Airspace System, U.S. Government Accountability Office, 2012. www.gao.gov/products/GAO-12-981

W. C. Bennett, *Unmanned at any speed : Bringing drones into our national airspace*, Issues in Governance Studies series, n° 55, Brookings Institution, 2012. www.brookings.edu/research/papers/2012/12/14-drones-bennett

O. Zubeldia, *Histoire des drones*, Perrin, 2012.