

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 malfaisance. 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.

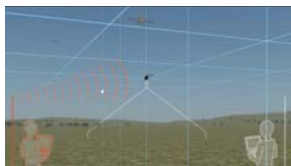
Pour l'Administration américaine de l'aviation, cette mission s'ajoute au développement d'un nouveau système de gestion du trafic aérien, le NextGen (*Next Generation Air Transportation System*). Les nouvelles réglementations devront instaurer un équilibre délicat entre les considérations de sécurité 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.