

Les DRONES menacés de piratage

Kyle Wesson et Todd Humphreys

Des flottilles d'avions sans pilote pourraient bientôt sillonner les airs, pour surveiller les feux de forêt, livrer des colis, réaliser des opérations de sauvetage, etc. Mais ces drones civils ont des failles de sécurité qui les rendent faciles à pirater.

Le 2 août 2010, un hélicoptère de reconnaissance de la marine américaine a pénétré dans l'espace aérien étroitement contrôlé qui s'étend autour de Washington. L'événement n'aurait mérité que quelques lignes dans le registre des contrôleurs aériens de l'aéroport voisin s'il n'y avait eu un détail troublant : l'hélicoptère n'avait pas de pilote. C'était un drone.

Le MQ-8B Fire Scout, un appareil de 1 429 kilogrammes et 9,7 mètres de long, a été victime d'un « problème de logiciel », selon les termes des enquêteurs. Il en a résulté une perte des communications avec les opérateurs qui le contrôlaient depuis une base aéronavale, éloignée de plusieurs dizaines de kilomètres. Et pour ne rien arranger, l'appareil n'a pas exécuté le programme censé le forcer à rentrer à la base dans ce cas de figure. Le drone s'est égaré dans le même espace aérien que celui utilisé par Air Force One, l'avion présidentiel, pour décoller et atterrir à la base militaire Andrews.

Après 30 minutes de tension, les opérateurs ont rétabli le contact et repris le

L'ESSENTIEL

■ **Des milliers d'avions sans pilote, ou drones, devraient bientôt effectuer des missions variées à des coûts réduits : sauvetage, surveillance des lignes électriques, recherche scientifique...**

■ **Leur déploiement dans l'espace aérien pose des problèmes de sécurité complexes et parfois sans réponse aujourd'hui.**

■ **Les signaux radio guidant et commandant les drones peuvent ainsi être falsifiés ou brouillés par des malfaiteurs souhaitant prendre le contrôle des appareils.**

Dan Winters

contrôle. Par la suite, un représentant de la marine a tenté de rester positif, en soulignant les bonnes performances du drone : ainsi, le système de pilotage automatique a maintenu l'appareil sur une trajectoire droite et horizontale.

Cette escapade imprévue doit nous alerter sur les immenses défis de sécurité que posent les drones. Ces systèmes de reconnaissance et de frappe commencent à être dédiés à toutes sortes de tâches civiles et plusieurs milliers d'entre eux pourraient survoler les États-Unis d'ici quelques années. Ils participeront peut-être bientôt aux opérations de recherche et de sauvetage, à la pulvérisation de pesticides, à la surveillance des lignes électriques, aux études scientifiques et à une multitude d'autres tâches.

En se passant de pilote – et de cockpit –, les compagnies qui déploient des drones espèrent faire des économies considérables. Par exemple, louer un avion piloté par un humain pour une campagne d'inspection des lignes électriques coûterait le même prix qu'acheter un véhicule aérien automatique susceptible de répéter ce travail un grand

nombre de fois. Les drones ont retenu l'attention des plus grosses entreprises. Frederick Smith, le fondateur et PDG de l'entreprise FedEx, spécialisée dans le transport international de fret, a évoqué le remplacement de sa flotte d'avions par des drones. En France, ERDF, le gestionnaire du réseau de distribution électrique, envisage d'en employer pour la surveillance des lignes.

Même le Congrès des États-Unis commence à admettre que les drones commerciaux vont se répandre. Dans une loi de 2012, il ordonnait l'établissement d'un « plan complet pour accélérer en toute sécurité l'intégration des systèmes civils d'aéronefs automatiques dans l'espace aérien national » d'ici 2015.

Malheureusement, les outils nécessaires à la gestion de ces robots télécommandés ont peu de chances d'être prêts à temps. Les drones étendent les responsabilités de l'Administration américaine de l'aviation au-delà de son rôle traditionnel, qui consiste à s'assurer que les avions restent à une distance respectable les uns des autres et résistent aux vicissitudes de la météo. À la suite des attaques du 11 septembre 2001, le rôle de cet organisme a été élargi aux problèmes de sécurité des avions, que l'arrivée d'essaims de drones dans le ciel multiplierait.

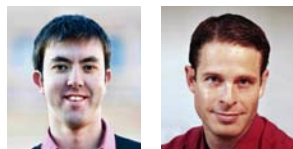
Trois types de liaisons nécessaires

Le plus grand défi est la sécurisation des liaisons sans fil des drones. Pour manœuvrer un appareil, trois liaisons principales sont nécessaires : la première avec les satellites de géolocalisation (le système GPS), la deuxième avec les autres aéronefs (qui doivent être avertis des déplacements du drone), et la troisième avec le sol (pour le pilotage de l'engin). La perturbation de l'une de ces trois liaisons peut avoir des conséquences catastrophiques. Dans certains cas, on ne dispose pas de solution technique pour les sécuriser.

Le GPS est le pilier du système de navigation d'un drone, qui comprend aussi des capteurs de guidage inertiel, des magnétomètres, des altimètres et des caméras. Parmi ces dispositifs, seul le récepteur GPS permet une navigation de précision constante. En outre, il n'est pas touché par les conditions météorologiques, à l'inverse des caméras.

Contrairement au GPS militaire, la version civile est librement accessible et non chiffrée. Disponible sur les téléphones por-

■ LES AUTEURS

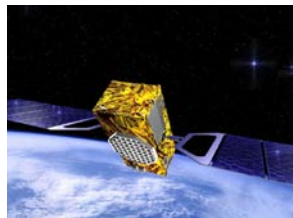


Kyle WESSON est doctorant en génie électrique et informatique à l'Université du Texas à Austin (États-Unis).

Todd HUMPHREYS est professeur de mécanique orbitale et directeur du Laboratoire de radio-navigation à l'Université du Texas.

Le guidage des drones par satellite

La géolocalisation par satellites (ci-dessous, un satellite du système européen Galileo, qui devrait être opérationnel d'ici un ou deux ans) est essentielle au pilotage des drones hors de la vue des opérateurs. En effet, lors d'un vol, la précision de la navigation fondée sur des cartes et des capteurs embarqués se dégrade au cours du temps. Un recalage périodique de la position est alors nécessaire. Toutes les procédures de sécurité, y compris celle qui force un drone à rentrer à sa base en cas de perte du signal de commande, utilisent un tel recalage, aujourd'hui par GPS.



tables ou les montres de sport, elle est très populaire, mais dépourvue de toute forme d'authentification, ce qui constitue une faiblesse dangereuse. On peut facilement remplacer le vrai signal par un faux (on parle de *spoofing*, ou de leurrage en français).

En juin 2012, dans la zone de tir de White Sands, au Nouveau-Mexique, notre équipe a montré que cela entraîne une menace pour les aéronefs sans pilote. Nous avons construit un dispositif de leurrage artisanal, qui a pris le contrôle d'un drone éloigné de 500 mètres. Notre dispositif émettait une imitation presque parfaite des signaux satellitaires qui relaient les coordonnées du drone jusqu'à lui. Incapable de distinguer entre le vrai et le faux signal, le drone s'est laissé guider par le plus intense, c'est-à-dire le nôtre.

Quand notre signal indiquait à tort au drone qu'il s'élevait verticalement, l'appareil descendait pour se maintenir à l'altitude programmée dans son système de pilotage automatique. Dès lors, il s'est rapproché dangereusement du sol. S'il ne s'est pas écrasé, c'est uniquement parce qu'un opérateur a fini par prendre le contrôle manuel de l'engin.

Le danger du leurrage est connu depuis plus d'une décennie. Le Département américain des transports l'a signalé dans un rapport de 2001, mais les décideurs et les fabricants d'appareils GPS n'en ont tenu compte que très récemment, pensant peut-être qu'une attaque était improbable. Les solutions techniques envisagées sont loin d'être prêtes. Certaines consistent à protéger les signaux GPS par crypto-tatouage (une signature numérique sécurisée qui identifie l'origine d'un signal et garantit le contenu de son message), mais elles ne pourront pas être implémentées avant plusieurs années. D'autres techniques se fondent sur des systèmes embarqués de supervision des mesures et de la navigation : ainsi, quand l'indication d'altitude donnée par le signal GPS n'est pas en accord avec les autres données (telle celles fournies par les altimètres et les caméras), ce signal n'est plus pris en compte. Cependant, ces techniques doivent encore faire leurs preuves.

Le leurrage n'est pas la seule menace qui pèse sur les drones dépendant des signaux GPS. Près de la surface de la Terre, ces signaux sont faibles et leur réception facile à bloquer : leur densité de flux (une mesure de la puissance du signal) équivaut à celle de la lumière émise par une ampoule