TRIBUNE LIBRE

Les drones dans le viseur des cybercriminels : que dit le droit ?

> par Jean-Baptiste Charles, avocat à la cour - Senior Associate, Hogan Lovells (Paris) LLP et Simon Parier, juriste - doctorant, Hogan Lovells (Paris) LLP - Université de Bordeaux (CERDI)

Aujourd'hui, l'informatique recèle une menace centrale : la cybercriminalité. Ce nouveau risque, protéiforme, figure en bonne place sur la cartographie stratégique du monde actuel, au même plan que le terrorisme qu'il sert d'ailleurs souvent. Dans son récent rapport prospectif (« Chocs futurs », mai 2017), le Secrétariat général de la défense et à la sécurité nationale (SGDSN) met en exergue la permanence de la conflictualité dans le cybermonde. Les objectifs des cybercriminels sont multiples : le gain financier, la déstabilisation des individus, entités et Etats, l'espionnage stratégique ou industriel, le sabotage, la manipulation et la spoliation des données.

LA FILIÈRE DU DRONE... UN SECTEUR PLUS QUE JAMAIS CONCERNÉ PAR LA CYBERCRIMINALITÉ.

Le secteur aéronautique dans son intégralité est concerné par cette menace, comme en témoigne le chiffre de 800 cyber-incidents enregistré par l'Air Traffic Organization pour l'année 2008, dont 17 % ne furent pas résolus. L'Organisation de l'Aviation civile internationale (« OACI ») a d'ailleurs adopté une résolution « A39-19 : Cybersécurité dans l'aviation civile » en octobre 2016 en prélude à une réglementation plus spécifique.


Simon Parier.

Les drones sont un moyen de mise en œuvre de cette menace contre les personnes, les Etats, les données, les systèmes d'information. Discrets et maniables, ils peuvent servir de relais et de vecteur de l'acte de cybercriminalité. Mais ces appareils (et les données qu'ils transportent) sont également de potentielles victimes et l'objet de l'attaque. Il est notamment possible d'en prendre le contrôle par l'exploitation de failles dans le protocole de communication et la réalisation d'interférences (exemple du boîtier Icarus) ou encore l'attaque des repères GPS du drone (GPS-spoofing).

Le rapport des Lloyds en 2015 (« Drones Take Flight ») souligne que les drones sont particulièrement vulnérables à de telles attaques. Cette étude révèle d'ailleurs qu'une communauté de hackers de drones se serait déjà constituée (activités de « drone hacking » et de « drone jacking »).

La filière des drones civils, qui connaît en France une croissance colossale depuis 2012 avec un chiffre d'affaires de 160 M€ et 10 000 emplois induits pour 2016, est donc confrontée à un enjeu crucial. Pour les spécialistes, le risque cyber est l'un des cinq obstacles majeurs auxquels la filière doit faire face.

UNE RÉPONSE ET DES MOYENS JURIDIQUES INSUFFISANTS.

La réglementation actuelle en matière de drones civils ne prévoit pas de dispositions particulières. Hormis le principe général de prudence qu'elle édicte – dont il peut se déduire une interdiction de commettre ou de participer à des cyberattaques – et l'interdiction faite aux exploitants et télépilotes de porter atteinte à la vie privée et aux données personnelles, le droit des drones est peu disert en matière de cyberattaques.

Le droit commun en matière de cybercriminalité l'est davantage, certains auteurs n'hésitant pas à le qualifier de « mille-feuilles » juridique. Il s'illustre effectivement par la pluralité des textes le constituant (plus de dix lois entre 2001 et 2016). A cet égard, le droit pénal de fond relatif aux cyberinfractions différera selon que le drone sera l'objet (ou la victime) de la cyberattaque ou son vecteur (ce que nous pourrions nommer le risque « v-v »). Les principales incriminations et infractions disponibles sont actuellement prévues par les articles 323-1 et suivants du Code pénal qui traitent des atteintes aux systèmes de traitement automatisé de données (« STAD »). Est notamment sanctionné à ce titre le fait d'accéder, de se maintenir frauduleusement dans tout ou partie d'un STAD ou encore d'en entraver, d'en perturber ou d'en fausser le fonctionnement.

D'autres textes (code de la défense, code de la sécurité intérieure, code des postes et des communications électroniques ; infractions prévues par la loi informatique et libertés, etc.) trouveront naturellement à s'appliquer.


Jean-Baptiste Charles.

Si les infractions existent, la règle d'interprétation stricte de la norme pénale risque toutefois de constituer une limite à l'extension des infractions existantes et à leur application aux drones civils. Très logiquement, opérationnels et praticiens appellent de leurs vœux l'adoption d'un arsenal répressif spécifique pour répondre à cette menace.

QUELLE ÉVOLUTION ?

L'évolution législative à venir devra prendre en compte les aspects classiques du droit pénal (notion de commission d'infractions en bande organisée, confiscations de moyens et de ressources, etc.) ainsi que les moyens d'action propres à la cyberdéfense (possibilité de « hack back » des autorités, etc.).

Cette évolution devra être mise en œuvre au sein du cadre existant en matière de drones civils en prévoyant notamment la sanction de l'utilisation d'un drone à des fins malveillantes, d'entrave, de perturbation ou de spoliation (entre autres) de STAD et de services automatisés.