NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME

5

Protéger les cibles vulnérables contre les attaques terroristes impliquant des systèmes de drone aérien

GUIDE DE BONNES PRATIQUES

Module spécialisé

Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables

En partenariat avec :
CONSEIL DE SÉCURITÉ DE L'ONU
DIRECTION EXÉCUTIVE DU COMITÉ CONTRE LE TERRORISME (DECT)
UNAOC United Nations Alliance of Civilizations
unicri United Nations Interregional Crime and Justice Research Institute

NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME

Protéger les cibles vulnérables contre les attaques terroristes impliquant des systèmes de drone aérien

GUIDE DE BONNES PRATIQUES
Module spécialisé

Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables

En partenariat avec : CONSEIL DE SÉCURITÉ DE L'ONU
DIRECTION EXÉCUTIVE DU COMITÉ CONTRE LE TERRORISME (DECT)
UNAOC United Nations Alliance of Civilizations
unicri United Nations Interregional Crime and Justice Research Institute

Table des matières

Préface v

Index des encadrés vii
Index des études de cas viii
Index des outils ix

1. La menace terroriste provenant des systèmes de drone aérien qui pèse sur les cibles vulnérables 1

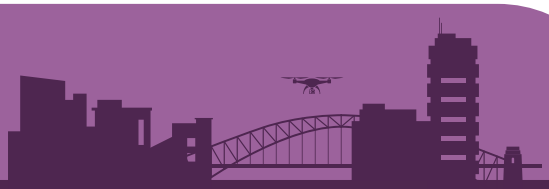
2. Exposition des cibles vulnérables aux attaques terroristes impliquant des systèmes de drone aérien 11

3. Atténuation des risques et intervention : rôles des parties prenantes et bonnes pratiques 14

3.1 États Membres 15
3.1.1 Décideurs 15
3.1.2 Forces de l'ordre 37
3.1.3 Services de renseignement 52

3.2 Acteurs non étatiques 54
3.2.1 Exploitants de cibles vulnérables 54
3.2.2 Fabricants de systèmes de drone aérien et de sous-systèmes essentiels 59
3.2.3 Vendeurs et détaillants de systèmes de drone aérien 64
3.2.4 Fournisseurs de technologies de lutte contre les systèmes de drone aérien 66
3.2.5 Utilisateurs de systèmes de drone aérien 66
3.2.6 Utilisateurs de cibles vulnérables 68
3.2.7 Organisations de la société civile 68

Références 70



Préface

Élaboré par le Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables du Bureau de lutte contre le terrorisme[1], le présent document se veut une source d'orientation concernant la protection des cibles vulnérables contre les attaques terroristes impliquant des systèmes de drone aérien. Ce module sectoriel complète le *Recueil des bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes*[2].

Après un survol des principales menaces et vulnérabilités liées aux attaques terroristes impliquant des systèmes de drone aérien, le présent module traite du rôle précis que chaque partie prenante peut et doit jouer dans un environnement de sécurité complexe – et souvent volatil –, à l'intérieur du cadre conceptuel de gestion des risques et des crises. Il contient des études de cas qui illustrent comment des gouvernements, des entités du secteur privé, des exploitants de sites vulnérables et des organisations de la société civile ont mis en œuvre des principes clés en matière de sécurité – y compris des recommandations approuvées par la communauté internationale. Le module résume également le contenu de plusieurs outils (manuels, guides et recueils) qui éclairent la mise en place de paramètres opérationnels et de politiques propres à rendre les cibles vulnérables plus résilientes et à faire en sorte qu'elles soient moins exposées aux attaques terroristes impliquant des systèmes de drone aérien.

Le cadre d'analyse, les études de cas, les outils et les ressources présentés dans ce module sont le fruit de recherches documentaires approfondies, d'une demande officielle de contributions auprès des 193 États Membres de l'Organisation des Nations Unies, de discussions avec des experts, des organisations internationales et des partenaires de projet individuels, ainsi que de la participation du Groupe de travail sur les nouvelles menaces et la protection des

1 Ayant pour partenaires la Direction exécutive du Comité contre le terrorisme, l'Alliance des civilisations de l'Organisation des Nations Unies et l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, le Programme est mis en œuvre en étroite consultation avec d'autres organisations concernées, telles qu'INTERPOL. Voir www.un.org/counterterrorism/fr/vulnerable-targets.

2 Le Recueil a été élaboré en 2018 par le Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme, sous la supervision de l'Équipe spéciale de lutte contre le terrorisme. En 2019, l'Équipe spéciale a été intégrée au Pacte mondial de coordination contre le terrorisme. Dans le cadre de cette nouvelle structure, ce Groupe de travail et le Groupe de travail sur la prévention des attentats terroristes à l'arme de destruction massive et les interventions en cas d'attentat ont été regroupés afin de créer le Groupe de travail sur les nouvelles menaces et la protection des infrastructures critiques.

infrastructures critiques du Pacte mondial de coordination contre le terrorisme[3]. Des renseignements importants ont été recueillis dans le cadre de deux réunions du Groupe d'experts organisées par le Bureau de lutte contre le terrorisme, auxquelles ont participé des experts d'États Membres, d'organisations internationales et régionales, de la société civile, du secteur privé et du milieu universitaire. La première réunion du Groupe d'experts a été tenue le 29 juin 2021, lors de la Semaine virtuelle de la lutte contre le terrorisme, et la deuxième s'est déroulée le 6 octobre 2021. Les contributions du conseiller pour les questions de genre du Bureau de lutte contre le terrorisme et d'un consultant spécialisé en droits humains du Service des projets spéciaux et de l'innovation du Bureau se sont également révélées profitables dans le cadre de ce processus.

Le présent module fait largement référence au document portant sur l'adoption de directives techniques visant à faciliter l'application de la résolution 2370 (2017) du Conseil de sécurité, des bonnes pratiques et des normes internationales connexes afin d'empêcher les terroristes d'acquérir des armes (ci-après dénommé « directives techniques pour l'application de la résolution 2370 du Conseil de sécurité »), dont le sous-module II porte sur les moyens d'empêcher les terroristes d'acquérir des systèmes de drone aérien ou leurs composants[4].

3 Voir www.un.org/counterterrorism/fr/global-ct-compact.

4 Voir www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf. En décembre 2021, les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité en étaient à la dernière étape de leur élaboration, qui s'inscrit dans un projet conjoint réalisé par la Direction exécutive du Comité contre le terrorisme, au nom du Groupe de travail sur la gestion des frontières et l'application de la loi du Pacte mondial de coordination contre le terrorisme. C'est le Centre des Nations Unies pour la lutte contre le terrorisme, qui relève du Bureau de lutte contre le terrorisme, qui finance ce projet et en assure la mise en œuvre avec l'Institut des Nations Unies pour la recherche sur le désarmement, en étroite collaboration avec les entités membres du Groupe de travail susmentionné.

Index des encadrés

Encadré 1.	**La menace que posent les systèmes de drone aérien et les agents chimiques, biologiques, radiologiques et nucléaires (CBRN) utilisés à des fins terroristes**	3
Encadré 2.	**Les systèmes de drone aérien comme cibles et vecteurs de cyberattaques**	6
Encadré 3.	**Vulnérabilités dans l'infrastructure informatique des systèmes de drone aérien**	13
Encadré 4.	**Stratégie pangouvernementale recommandée par l'OACI pour les systèmes de drone aérien**	19
Encadré 5.	**Gestion du trafic des systèmes de drone aérien**	24
Encadré 6.	**Difficultés en vue pour la coopération internationale dans la lutte contre les systèmes de drone aérien utilisés à des fins terroristes**	34
Encadré 7.	**Le respect des droits humains et des libertés fondamentales dans les opérations de maintien de l'ordre faisant appel aux systèmes de drone aérien**	37
Encadré 8.	**Intégration des informations recueillies à l'aide des systèmes de drone aérien dans le travail des centres de centralisation du renseignement**	40
Encadré 9.	**Systèmes de drone aérien et raids jusqu'au point d'origine**	43
Encadré 10.	**Le danger potentiel des systèmes de drone aérien retrouvés au sol – nord de l'Iraq**	48
Encadré 11.	**La conspiration des entreprises IBACS – plusieurs pays**	49
Encadré 12.	**Réseau de fournisseurs de systèmes de drone aérien de Daech**	53
Encadré 13.	**Les fabricants de systèmes de drone aérien et les solutions de géoblocage**	60
Encadré 14.	**Signaux d'alarme et manque de diligence dans l'affaire des entreprises IBACS**	64
Encadré 15.	**Services de systèmes de drone aérien à la demande**	68

Index des études de cas

Étude de cas 1.	**Stratégie de l'Union européenne pour lutter contre les systèmes de drone aérien en contexte antiterroriste**	20
Étude de cas 2.	**UK Counter-Unmanned Aircraft Strategy (Stratégie du Royaume-Uni pour lutter contre les drones aériens)**	21
Étude de cas 3.	**L'approche de Singapour face aux risques de sécurité posés par les systèmes de drone aérien**	22
Étude de cas 4.	**Cadre de réglementation des systèmes de drone aérien de l'Union européenne**	25
Étude de cas 5.	**Cadre de gestion des risques des Émirats arabes unis concernant les aéronefs non autorisés dans l'espace aérien contrôlé**	26
Étude de cas 6.	**Projet Courageous : méthodologie permettant de choisir la bonne technologie pour lutter contre les systèmes de drone aérien**	28
Étude de cas 7.	**Programme de financement de l'accélérateur de défense et de sécurité (Defence and Security Accelerator) – Royaume-Uni**	29
Étude de cas 8.	**Portail de ressources « Sécurité des drones »**	30
Étude de cas 9.	**Utilisation des systèmes de drone aérien pour prévenir les attaques terroristes – Costa Rica**	36
Étude de cas 10.	**Mise à l'essai et évaluation des contre-mesures visant les drones – INTERPOL et police norvégienne**	44
Étude de cas 11.	**Utilisation des systèmes de drone aérien par la police de la Catalogne (Espagne)**	45
Étude de cas 12.	**Pouvoir d'interpellation et de fouille à l'égard des systèmes de drone aérien**	50
Étude de cas 13.	**Association des exploitants de drones commerciaux de l'Afrique australe (Commercial Unmanned Aircraft Association of Southern Africa – CUAASA)**	61
Étude de cas 14.	**Groupe d'action du secteur des drones (Drone Industry Action Group – Drone IAG)**	62
Étude de cas 15.	**Détection des vulnérabilités : programme de prime aux bogues**	63

Étude de cas 16. **Programme de certification Dronesafe pour les détaillants du Royaume-Uni** 65

Étude de cas 17. **Drones Sans Frontières** 69

Index des outils

Outil 1. **The Islamic State and Drones: Supply, Scale, and Future Threats (L'État islamique et les systèmes de drone aérien : approvisionnement, étendue du problème et menaces futures) – Combating Terrorism Center at West Point (2018)** 8

Outil 2. **How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools (Comment analyser la cybermenace provenant des systèmes de drone aérien : contexte, cadres analytiques et outils d'analyse) – Rand Corporation (2020)** 9

Outil 3. **Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités – Forum mondial de lutte contre le terrorisme (2019)** 15

Outil 4. **Trousse d'outils de l'Organisation de l'aviation civile internationale (OACI) pour les UAS** 17

Outil 5. **Model UAS Regulations (modèle de réglementation des UAS) – OACI** 27

Outil 6. **Communication avec l'extérieur : information et sensibilisation – trousse d'outils de l'OACI pour les UAS** 31

Outil 7. **Bonnes pratiques et mesures de sécurité pour le déploiement de technologies de lutte contre les systèmes de drone aérien – Ministère des transports du Royaume-Uni (2018)** 46

Outil 8. **Counter-Unmanned Aircraft Systems: Technology Guide (Guide sur les technologies de lutte contre les systèmes de drone aérien) – Département de la sécurité intérieure des États-Unis (2019)** 47

Outil 9. **Counter-Drone Systems (Systèmes anti-drones) – Center for the Study of the Drone du Bard College (2019)** 47

Outil 10. **Cadre d'intervention en cas d'incident lié à un drone : À l'intention des premiers intervenants et des professionnels de la criminalistique numérique – INTERPOL (2020)** 51

Outil 11. **État du contexte de risque mondial de sûreté de l'aviation civile, Doc 10108 – OACI** 56

Outil 12. **Drone Incident Management at Aerodromes (Gestion des incidents de drones dans les aérodromes) – Agence européenne de la sécurité aérienne (2021)** 57

Outil 13. **Protecting Against the Threat of Unmanned Aircraft Systems (UAS) : An Interagency Security Committee Best Practice (Protection contre la menace des systèmes de drone aérien : meilleures pratiques) – Département de la sécurité intérieure des États-Unis (2020)** 58

Outil 14. **Countering Threats from Unmanned Aerial Systems: Making Your Site Ready (Contrer les menaces des systèmes de drone aérien : comment préparer votre site) – Centre for the Protection of National Infrastructure du Royaume-Uni (2020)** 59

[1]

La menace terroriste provenant des systèmes de drone aérien qui pèse sur les cibles vulnérables

Les drones aériens sont des aéronefs qui peuvent fonctionner sans pilote à bord. Ils constituent l'élément aérien mobile des systèmes de drone aérien (UAS), qui comprennent également un système de contrôle au sol et des charges utiles[5].

Les systèmes de drone aérien comprennent divers modes de navigation aérienne[6], qui les rendent autonomes à différents degrés. Leur taille, leur poids, leur forme et leur prix sont des plus variés, tout comme l'équipement technologique connexe. Ils peuvent être conçus et utilisés aussi bien dans le domaine civil que militaire. Parmi ceux dont l'utilisation relève du domaine civil, on retrouve les drones de loisir, conçus pour les amateurs, et ceux utilisés à des fins professionnelles. Ces derniers permettent toute une gamme d'applications – qui ne cesse de s'élargir – comprenant notamment la surveillance et le traitement des cultures, les inspections industrielles et

5 Voir les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité, sous-module II, section 1.1.1 sur les composants des systèmes de drone aérien.

6 Les modes de navigation de base des systèmes de drone aérien sont les suivants : 1) la navigation manuelle, qui repose sur la communication radio entre le drone et le système de contrôle au sol; 2) la navigation GPS, qui ne dépend pas des signaux radio et qui permet de préprogrammer les drones pour qu'ils volent de manière autonome jusqu'à des endroits précis ou selon des tracés prédéterminés; 3) la navigation autonome, qui fait appel aux capteurs internes du drone, lesquels permettent à l'appareil de suivre des objets ou des personnes en mouvement ou de viser des objets immobiles.

les opérations de sauvetage et de secours en cas de catastrophe.

Les UAS continuent de bénéficier d'un essor technologique[7] et des avancées théoriques et pratiques en intelligence artificielle[8]. En outre, de nombreux UAS vendus sans restriction peuvent être facilement modifiés ou améliorés pour répondre à des besoins individuels. On peut aussi acheter des pièces séparément et les assembler pour créer un « UAS sur mesure » qui répondra à un ou des besoins particuliers.

Bien que les UAS contribuent manifestement à la sécurité et au développement des pays à plusieurs égards, ils créent aussi de nouvelles possibilités d'attentat terroriste. La précision et la fiabilité croissantes de ces appareils, de même que la facilité avec laquelle il est possible d'y intégrer des fonctions personnalisées sont généralement utilisées à bon escient, mais elles peuvent aussi servir un dessein criminel ou terroriste.

Le Conseil de sécurité a déjà demandé que des mesures soient prises afin d'atténuer le risque que des UAS soient exploités à des fins terroristes. Dans la résolution 2370 (2017)[9], plus particulièrement, il « condamn[e] fermement la circulation continue d'armes, notamment d'armes légères et de petit calibre, de matériel militaire, de drones et d'engins explosifs improvisés, et de leurs pièces détachées entre l'État islamique d'Iraq et du Levant (EIIL, également connu sous le nom de Daech), Al-Qaida, les éléments qui leur sont affiliés, les groupes qui leur sont associés et les groupes armés illicites et les criminels, ou à destination de ces entités, et encourag[e] les États Membres à prévenir et démanteler les réseaux d'achat de ces armes, systèmes et pièces détachées ».

Dans l'actuel contexte mondial de sécurité, un certain nombre de facteurs concomitants semblent contribuer au risque que des groupes terroristes acquièrent des UAS et développent l'expertise nécessaire pour les employer efficacement. Ces facteurs comprennent notamment[10] : 1) le marché civil non réglementé de technologies d'UAS de plus en plus avancées; 2) la grande accessibilité d'explosifs non réglementés, non contrôlés et non sécurisés, qui peuvent être utilisés comme charges utiles sur les UAS; 3) l'accès aux précurseurs d'explosifs (nitrate d'ammonium, peroxyde, etc.); 4) l'expertise technique dont disposent les terroristes et les personnes ou groupes associés, et le transfert de cette expertise.

Les observations qui précèdent ne suggèrent pas forcément que les UAS deviendront dans un avenir prévisible le vecteur le plus utilisé ou le plus courant pour mener des attaques terroristes. Toutefois, de plus en plus d'éléments indiquent que des acteurs non étatiques tentent d'en tirer parti pour servir des objectifs terroristes bien au-delà des zones visées par des opérations militaires. Ce phénomène accroît fortement le risque que des attaques soient menées contre les infrastructures critiques et autres cibles vulnérables.

---

7 La forte demande sur le marché a stimulé le développement de capteurs de plus en plus sophistiqués, de l'automatisation, de batteries offrant une plus grande autonomie, etc. Compte tenu du rythme soutenu des innovations dans ce secteur, les UAS sont rapidement surpassés par les nouvelles générations.

8 Les UAS dotés d'intelligence artificielle constitueraient de fait des systèmes d'armes autonomes capables de rechercher, choisir et attaquer des cibles par eux-mêmes. Il est possible que de tels systèmes aient déjà été déployés en Libye lorsque les « convois de logistique et les unités des forces affiliées à Haftar qui battaient en retraite ont été pourchassés et pris à partie à distance par des drones de combat ou des systèmes d'armes létaux autonomes [...] et d'autres munitions rôdeuses. Les systèmes d'armes létaux autonomes avaient été programmés pour attaquer des cibles, sans qu'il soit besoin d'établir une connexion des données entre l'opérateur et la munition, et étaient donc réellement en mode d'autoguidage automatique. » (S/2021/229, par. 63.)

9 Une disposition identique est comprise dans d'autres instruments publiés ultérieurement par le Conseil de sécurité, dont la résolution 2482 (2019).

10 Activité parallèle organisée par le Bureau de lutte contre le terrorisme le 29 juin 2021 (Semaine virtuelle de la lutte contre le terrorisme).

Encadré 1.
La menace que posent les systèmes de drone aérien et les agents chimiques, biologiques, radiologiques et nucléaires (CBRN) utilisés à des fins terroristes

Les acteurs hostiles qui souhaitent provoquer un incident chimique, biologique, radiologique ou nucléaire (CBRN) peuvent se servir d'UAS comme vecteurs pour propager les agents CBRN qu'ils transportent[11] ou comme armes pour attaquer une installation CBRN.

Le premier événement enregistré où des acteurs non étatiques ont cherché à combiner l'utilisation d'agents CBRN à celle d'un UAS à des fins terroristes remonte à 1994, lorsque la secte millénariste Aum Shinrikyo a tenté sans succès d'utiliser deux hélicoptères télécommandés pour répandre du gaz sarin. En 2015, un homme a réussi à faire voler un drone transportant du sable radioactif jusque sur le toit du bureau du Premier Ministre japonais. Fait crucial, le drone n'a été découvert que par hasard, quelques jours plus tard. L'année suivante, le Premier Ministre britannique de l'époque a signalé que les éléments affiliés à l'EIIL/Daech prévoyaient de mener des attaques à la bombe « sale » en libérant des agents nucléaires transportés par UAS au-dessus de zones urbaines densément peuplées.

En 2019, l'Unité de coordination de la lutte antiterroriste de la France a publié un rapport confidentiel prévenant d'une éventuelle attaque terroriste contre un stade de football au moyen d'un drone sans pilote équipé d'agents de guerre biologiques. Cette mise en garde a été réitérée par le Commissaire européen chargé de l'Union de la sécurité[12].

11 Par exemple, des UAS conçus pour un usage agricole (notamment pour épandre des pesticides dans les champs) peuvent devenir des vecteurs utilisés pour propager des agents CBRN.

12 La menace que représentent les UAS pour les spectateurs et les athlètes, en particulier lors de compétitions sportives enregistrant une forte affluence, est mentionnée dans le *Guide sur la sécurité des grandes manifestations sportives*, publié en 2021 par le Bureau de lutte contre le terrorisme, l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, l'Alliance des civilisations de l'ONU et le Centre international pour la sécurité dans le sport (disponible en anglais à l'adresse www.unaoc.org/wp-content/uploads/GUIDE-on-MSE-Security-with-Annex-Final.pdf, p. 36).

(suite)

La menace est considérée comme potentiellement grave, compte tenu des conséquences disproportionnées que pourrait avoir une seule tentative réussie. En outre, bien qu'une attaque CBRN par UAS ne cause pas nécessairement beaucoup de blessures aux victimes, son impact psychologique sur le public serait considérable. Même des agents non létaux peuvent provoquer une grande panique, ce qui serait notamment le cas si plusieurs UAS libéraient des substances toxiques au-dessus d'un stade[13]. De plus, des opérations de nettoyage vraisemblablement très coûteuses devraient être menées à grande échelle à la suite d'une telle attaque, et les premiers secours et les services de sauvetage pourraient avoir beaucoup plus de difficultés à enlever les débris, effectuer des recherches et reconstruire les infrastructures en raison des niveaux de contamination[14].

La possibilité que des acteurs non étatiques utilisent des UAS pour livrer des armes CBRN est envisagée dans le cadre juridique international actuel, et les États Membres sont invités à adopter des mesures de contrôle appropriées. Dans sa résolution 1540 (2004), le Conseil de sécurité a notamment décidé que tous les États devaient adopter et appliquer une législation appropriée et efficace interdisant à tout acteur non étatique de fabriquer, se procurer, mettre au point, posséder, transporter, transférer ou utiliser des armes nucléaires, chimiques ou biologiques ou leurs vecteurs.

Comme les UAS sont des vecteurs, la résolution 1540 peut être considérée comme un outil à part entière exigeant des pays qu'ils endiguent la prolifération des UAS pouvant être utilisés pour commettre des actes terroristes impliquant des armes CBRN.

Au cours des dernières années, les forces de l'ordre ont détecté ou déjoué divers plans liés au terrorisme qui reposaient sur l'utilisation d'UAS dans des zones exemptes de conflits[15]. En voici quelques exemples :

- Pendant les Jeux olympiques de 2016 à Rio de Janeiro, des agents d'Al-Qaida ont donné l'ordre de cibler des athlètes et des spectateurs. La police brésilienne aurait arrêté le lendemain un groupe de dix suspects en lien avec cette information [Moore (2016)];
- En 2019, en banlieue de Jakarta, un groupe de militants a été trouvé en possession d'un UAS et de batteries. L'année suivante, la police antiterroriste indonésienne a procédé à une série d'arrestations qui ont permis de mettre au jour l'intention du groupe d'utiliser des drones à des fins terroristes [Association of the United States Army (2021)];
- En septembre 2020, une cour d'appel danoise a confirmé les verdicts de culpabilité rendus par un tribunal de première

13 Observations de M. Günter Povoden, Consultant principal à l'Office des Nations Unies contre la drogue et le crime, lors de la réunion du Groupe d'experts sur la protection des cibles vulnérables et les UAS, organisée par le Bureau de lutte contre le terrorisme les 6 et 7 octobre 2021.

14 Pour une analyse générale des problèmes que les acteurs non étatiques peuvent rencontrer lorsqu'ils utilisent des UAS pour répandre des agents CBRN, voir l'exposé de Philipp C. Bleek sur les menaces de terrorisme liées aux drones et aux agents CBRN et les façons d'y répondre, présenté lors de la conférence « Countering Drones 2020 » organisée par Defense iQ le 4 juin 2020 (www.middlebury.edu/institute/news/drones-and-cbrn-terrorism-threats-and-responses).

15 Don Rassler a dressé une liste exhaustive des complots terroristes présumés impliquant des UAS jusqu'à la fin de 2016. Il établit notamment une distinction entre les entités terroristes qui ont manifesté un intérêt plus limité pour les UAS et celles dont l'utilisation des drones est suffisamment soutenue et avancée pour être considérée comme un « programme » [Rassler (2016)].

instance à l'encontre de trois personnes reconnues coupables d'avoir défendu et soutenu Daech[16]. Europol précise notamment dans son rapport que les hommes avaient acheté des drones de loisir ainsi que des pièces détachées, qui devaient être utilisés dans le cadre des activités et du programme de drones de Daech liés aux affrontements en Syrie et en Iraq (Europol (2021), p. 37).

Le retour des combattants terroristes étrangers de République arabe syrienne ou d'Iraq a suscité des préoccupations quant à la possibilité que les éléments affiliés à l'EIIL/Daech planifient le transfert dans leur pays d'origine des technologies et des tactiques liées aux UAS apprises sur le champ de bataille[17] [Forum mondial de lutte contre le terrorisme (2019)].

Les UAS offrent aux groupes terroristes différents avantages stratégiques, le plus important étant la possibilité accrue de contourner les mesures de protection physique traditionnelles fondées sur des niveaux de sécurité multiples (comme les périmètres des sites renforcés afin de freiner les attaques en voiture, les gardes armés ou les barrières pour le contrôle des visiteurs).

Celles et ceux qui utilisent des UAS peuvent également mener leurs activités depuis des endroits cachés ou protégés, ce qui réduit le risque que les contre-mesures prises les atteignent. Les technologies permettant le pilotage d'UAS au-delà de la visibilité directe sont désormais couramment utilisées dans diverses applications commerciales et gouvernementales. Employées à des fins illicites, notamment dans le cadre d'activités terroristes, ces technologies rendent plus difficile pour les forces de l'ordre de repérer et d'appréhender les pilotes de drones. En outre, les UAS équipés de caméras permettent aux terroristes potentiels de maximiser l'impact médiatique de leurs actes, par exemple en diffusant des images en direct de leurs attaques aériennes sur les plateformes de médias sociaux[18].

16 La dernière décision judiciaire rendue dans cette affaire a été portée en appel devant la Cour suprême du Danemark.

17 Dans le Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, on fait observer que « l'EIIL/Da[ech] a très souvent recouru à des systèmes d'aéronefs non habités pour commettre des attentats, effectuer des opérations de surveillance et mener sa propagande sur le champ de bataille en Ira[q] et en Syrie » et que « [l]es connaissances et l'expérience ainsi acquises peuvent ensuite être rapportées depuis ces zones par les combattants terroristes étrangers ou servir de modèles à des terroristes d'origine nationale, y compris ceux agissant seuls ».

18 Les experts en sécurité envisagent également des scénarios dans lesquels des groupes terroristes intègrent aux UAS des logiciels de reconnaissance faciale pour permettre des assassinats ciblés ou des logiciels conçus pour estimer la taille d'une foule afin de faire plus de victimes (Don Rassler, réunion du Groupe d'experts du Bureau de lutte contre le terrorisme tenue les 6 et 7 octobre 2021).

Encadré 2.
Les systèmes de drone aérien comme cibles et vecteurs de cyberattaques

Les UAS peuvent être des cibles ou des vecteurs de cyberattaque ou de piratage.

- **Les UAS comme cibles :** les terroristes peuvent chercher à prendre le contrôle d'un UAS dans le but de s'en emparer, de le détruire, d'en modifier la trajectoire ou d'en compromettre les données[19]. Par exemple, de fausses informations peuvent être transmises au système GPS d'un UAS pour l'amener à croire qu'il suit l'itinéraire prévu. Les failles logicielles doivent être décelées et corrigées régulièrement, car les terroristes risquent de les exploiter pour accéder à des UAS légalement immatriculés et exploités, y compris ceux utilisés dans le cadre des missions gouvernementales et de maintien de l'ordre. Les terroristes pourraient alors prendre le contrôle d'un UAS officiel et l'utiliser contre le site vulnérable ou très fréquenté qu'il était censé protéger.
- **Les UAS comme vecteurs :** les terroristes peuvent chercher à exploiter les UAS pour mener des cyberattaques contre d'autres types de cibles. Les UAS sont alors employés comme cyberarmes pour implanter des logiciels malveillants dans d'autres systèmes, tels que les infrastructures d'information critiques. La technologie 5G étant désormais la nouvelle norme pour les réseaux cellulaires à large bande, il est possible que le signal de communication des UAS devienne un outil plus facile à utiliser pour perturber les communications sans fil privées.

Source : Ley Best *et al.* (2020).

19 En 2009, à l'aide d'un logiciel vendu sur Internet au coût de 26 dollars, des rebelles en Iraq ont réussi à accéder à des UAS américains et à intercepter les retransmissions vidéo en direct relayées à un poste de contrôle américain, découvrant ainsi des cibles potentielles. Le piratage n'a été découvert qu'après que les États-Unis eurent obtenu l'accès aux ordinateurs portables des activistes, qui contenaient des heures d'enregistrements vidéo.

Les groupes terroristes peuvent avoir recours à des UAS pour atteindre différents objectifs[20]. Ils peuvent notamment les utiliser contre des cibles vulnérables aux fins suivantes :

- *Renseignement, surveillance et reconnaissance :* on peut déployer des UAS pour se renseigner sur les points faibles de certains sites, qui ne sont peut-être pas visibles depuis le sol, dans l'intention de les exploiter en menant une attaque par drone ou par des moyens conventionnels;
- *Attaque :* les UAS peuvent être utilisés pour percuter une cible dans le but de faire des victimes et de causer des dommages matériels, ou pour lancer des engins explosifs[21] ou libérer des agents CBRN (voir encadré 1). Leurs signaux de communication peuvent aussi servir, par exemple, à activer des brouilleurs de fréquences radio pour interférer avec les signaux utilisés par le personnel de sécurité pendant le déroulement d'un grand événement. L'impact des UAS employés comme armes est d'autant plus grand lorsqu'ils sont utilisés en grand nombre. Bien qu'en général, les UAS nécessitent encore tous leur propre pilote, le lancement simultané d'un grand nombre d'appareils formant une flotte imposante aux déplacements coordonnés est un scénario de plus en plus vraisemblable[22];
- *Propagande :* les terroristes peuvent utiliser des UAS pour filmer leurs attaques contre des sites vulnérables ou très fréquentés et diffuser ensuite des images choquantes dans le but de maximiser la couverture médiatique. L'utilisation des UAS aux fins de propagande est une des caractéristiques de la stratégie relative aux drones de Daech[23];

20 Voir les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité, sous-module II, section 1.1.3 sur l'utilisation des UAS à des fins terroristes.

21 En août 2018, le Président vénézuélien Nicolás Maduro a été la cible d'une tentative d'assassinat manquée au moyen de deux UAS guidés par GPS qui étaient chargés d'explosifs. En outre, l'EIIL/Daech a employé à plusieurs reprises des UAS dans des zones de conflit pour larguer des petites bombes de la taille de grenades. Bien que l'utilisation de ces appareils n'ait pas changé l'issue du conflit, elle a mis en évidence les conséquences potentiellement mortelles des UAS rudimentaires conçus pour le grand public, s'ils sont utilisés à mauvais escient.

22 Un tel cas s'est produit en 2018 lorsque deux des bases aériennes de la Fédération de Russie en République arabe syrienne ont été attaquées par une flotte de 13 UAS contrôlés par GPS qui étaient chargés d'explosifs et dont les déplacements étaient coordonnés. Ni le point de lancement ni les personnes à l'origine de l'attaque n'ont pu être identifiés.

23 En plus de transformer les UAS en armes, Daech s'en sert d'outils stratégiques pour produire des images venant alimenter son impressionnante machine de propagande.

- *Perturbation de service ou d'événement :* même lorsque les UAS ne sont pas employés comme armes, leur utilisation dans un espace aérien contrôlé ou restreint peut gravement perturber le fonctionnement des services gouvernementaux, des infrastructures critiques, des grands événements, etc. Ces dernières années, plusieurs UAS détectés à proximité ou à l'intérieur du périmètre de différents aéroports dans le monde sont venus perturber l'aviation civile et ont entraîné des pertes et des répercussions économiques assez considérables[24]. En aucun cas, il n'a été possible de prêter des visées terroristes aux incidents signalés liés à l'utilisation non autorisée d'UAS, et l'on peut affirmer sans présomption que la plupart de ceux-ci résultaient soit de la négligence ou de l'imprudence des pilotes, soit de leur intention de défier les règles pour attirer l'attention des médias.
- *Exposition ou renforcement de la vulnérabilité des cibles :* il ne peut être exclu que des UAS soient utilisés à seule fin de détourner l'attention et les moyens des forces de l'ordre et du personnel de sécurité de la cible véritable. Laissée sans protection et plus vulnérable, celle-ci peut ensuite faire l'objet d'une attaque par des moyens conventionnels ou des UAS armés.

Outil 1.
The Islamic State and Drones: Supply, Scale, and Future Threats (L'État islamique et les drones : approvisionnement, étendue du problème et menaces futures) – Combating Terrorism Center at West Point (2018)
(https://ctc.usma.edu/islamic-state-drones-supply-scale-future-threats)

Ce rapport examine comment Daech a réussi à mettre sur pied son programme de drones en relativement peu de temps et à utiliser efficacement des UAS commerciaux modifiés pour servir d'armes. Il fait état de quelques menaces et incidences politiques plus générales associées à l'utilisation inédite des UAS par Daech et explique notamment comment son modèle pourrait inspirer d'autres acteurs cherchant à développer leurs propres capacités et stratégies de guerre hybride.

Le rapport décrit comment les pays pourraient cibler les UAS utilisés à des fins terroristes et éviter de les rendre accessibles. On y donne notamment les conseils suivants :

- Se montrer plus prudents à l'égard des transactions qui requièrent l'expédition aux abords d'une zone de guerre complexe;
- Si la diligence voulue ne peut être exercée, s'assurer d'avoir accès à un gouvernement ou à une tierce partie neutre qui pourrait fournir une assistance semblable;
- Travailler avec l'industrie pour renforcer le suivi ou le retraçage des UAS commerciaux et leur emballage, une fois que les appareils ou leurs composants ont été récupérés dans des zones de conflit;
- Consacrer plus de temps et de ressources aux efforts visant à empêcher la livraison de certains articles à double usage dans les principales zones de conflit;
- Enquêter sur les réseaux d'approvisionnement et les cartographier;
- Retracer des équipements particuliers, comme les drones, trouvés sur le terrain pour stopper plus rapidement les filières d'approvisionnement existantes.

24 Le public a pris conscience de ce problème lorsque l'unique piste de l'aéroport de Londres Gatwick a été fermée du 19 au 21 décembre 2018 en raison de la présence de 115 drones. Dans l'ensemble, la perturbation engendrée a entraîné l'annulation de plus de 1 000 vols et touché quelque 140 000 passagers. Depuis, de nombreux aéroports dans le monde ont connu des perturbations causées à différents degrés par la présence de drones.

Outil 2.
How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools (Comment analyser la cybermenace provenant des systèmes de drone aérien : contexte, cadres analytiques et outils d'analyse) – Rand Corporation (2020)
(www.rand.org/pubs/research_reports/RR2972.html)

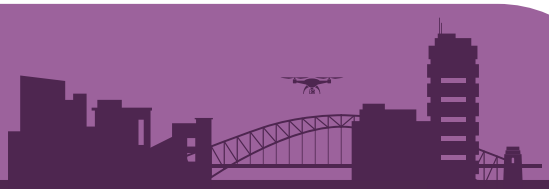
Cet outil propose un cadre conceptuel permettant de classer les cybermenaces liées aux UAS et couvre aussi bien l'utilisation de tels systèmes comme cibles que comme vecteurs de cyberattaques. Dans le but d'illustrer l'éventail des menaces qui se profilent actuellement, les cyberattaques impliquant des UAS sont classées suivant l'acronyme anglais S.T.R.I.D.E. :

- **S – « Spoofing » (usurpation) :** violation des protocoles d'authentification permettant à un attaquant de se faire passer pour une autre personne ou une autre entité. Lorsqu'un UAS sert de cible, l'usurpation peut consister à prétendre être le destinataire des données qu'il transmet;
- **T – « Tampering » (modification non autorisée) :** violation de l'intégrité d'un système en y apportant une modification quelconque; par exemple, utiliser un UAS pour se rendre à proximité d'un ordinateur cible et y implanter un logiciel malveillant depuis un réseau sans fil non sécurisé;
- **R – « Repudiation » (répudiation) :** les attaquants refusent d'assumer la responsabilité d'une action. Par exemple, la répudiation permet aux personnes qui utilisent un UAS comme cyberarme de se dissocier des conséquences d'une attaque en interférant au niveau du nœud de communications associé au point de dommage ou de perturbation;

(suite)

- **I – « Information » :** violation du principe de confidentialité; par exemple, infiltrer le système de données d'un capteur d'UAS pour accéder à des données vidéo, audio ou autres;
- **D – « Denial of service » (déni de service) :** par exemple, pirater les logiciels de contrôle de drones afin que les appareils ne répondent plus aux commandes du pilote;
- **E – « Elevation of privilege » (élévation de privilèges) :** violation du principe d'autorisation à exécuter une action donnée; par exemple, détourner un UAS en se faisant passer pour la personne qui le contrôle légitimement.

[2]



Exposition des cibles vulnérables aux attaques terroristes impliquant des systèmes de drone aérien

Les pays rencontrent souvent des problèmes lorsqu'ils tentent de protéger les personnes et les biens contre le risque d'attaques terroristes impliquant des UAS qui pèse sur les sites extérieurs où se rassemblent de grandes foules (manifestations sportives, religieuses ou culturelles; attractions touristiques; etc.). Ces problèmes sont notamment les suivants :

- *Faible reconnaissance de la nature et de l'ampleur de la menace :* pour plusieurs des cibles extérieures jugées vulnérables, la menace provenant des UAS n'a pas encore été pleinement prise en compte dans les plans de sécurité élaborés. Les sites où l'on se fie exclusivement aux plans de sécurité visant à endiguer la menace d'attaques terrestres, navales ou cybernétiques peuvent rester exposés aux incursions aériennes au moyen d'UAS. Éliminer des vulnérabilités peut inciter les acteurs terroristes à exploiter les autres points faibles qui n'ont pas encore été corrigés.

  Au cours d'une crise, les forces de l'ordre et le personnel de sécurité ont souvent la difficile tâche d'évaluer la motivation de l'incident impliquant un UAS. Bien que le choix d'intervention repose sur la capacité à distinguer les actes de négligence des actes de malveillance, le peu d'informations disponibles, les signalements contradictoires et la nécessité d'agir avec célérité rendent souvent cette distinction particulièrement difficile.

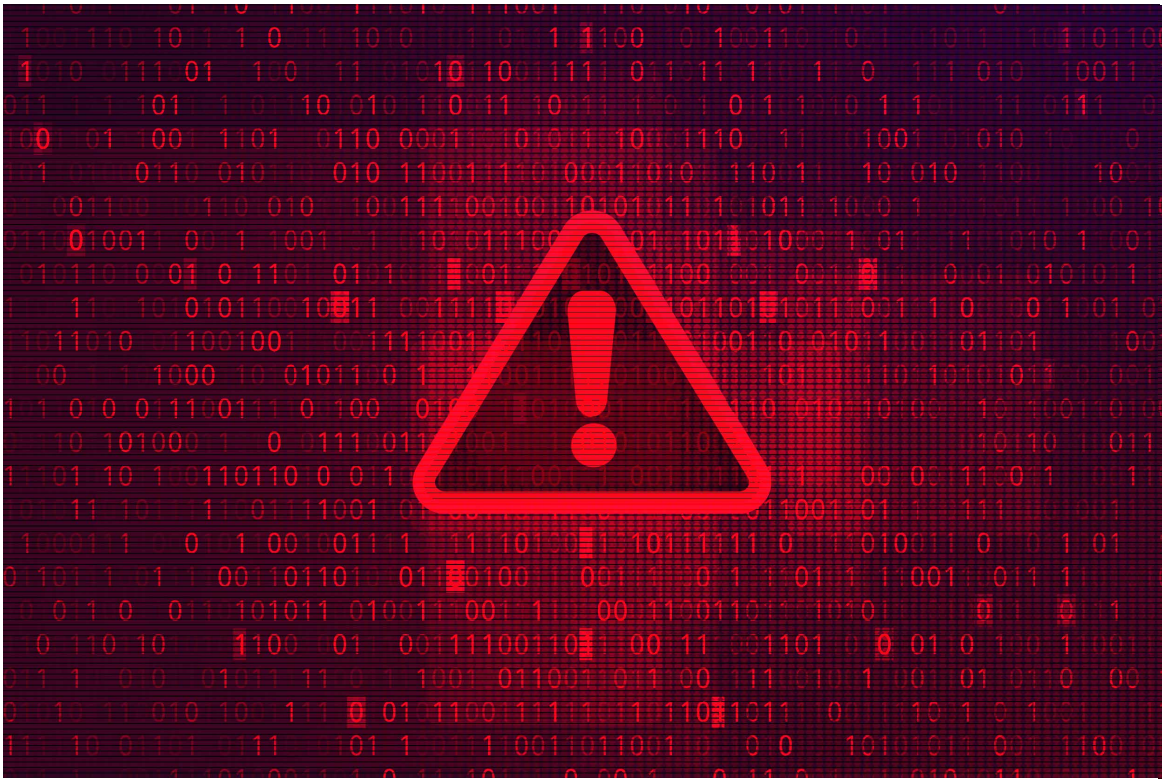
- *Cadres réglementaires inadéquats :* les cadres réglementaires nationaux, y compris ceux visant à protéger les cibles vulnérables contre les attaques par UAS, sont encore rudimentaires, voire inexistants. De plus, le marché évolue beaucoup plus rapidement que la réglementation applicable. Dans de nombreux pays, il reste plusieurs questions essentielles à régler afin de trouver un juste équilibre entre la nécessité de reconnaître et de promouvoir les utilisations légitimes des UAS et celle d'empêcher leur exploitation abusive. Il faut notamment donner les moyens aux forces de l'ordre et autres autorités étatiques d'agir en cas d'utilisation d'UAS à des fins hostiles, et créer des mesures afin d'inciter les exploitants de sites vulnérables à renforcer la sécurité anti-attaque par UAS, notamment par la création de partenariats public-privé. Les pays dotés d'un cadre réglementaire peuvent être appelés à clarifier les pouvoirs non définis ou à assigner les compétences dans des contextes souvent complexes où plusieurs organismes interagissent, tandis que ceux qui ont peu ou pas de règlements concernant les UAS doivent se familiariser avec ce type de réglementation et l'intégrer.

- *Non-disponibilité de technologies anti-UAS ou difficultés liées à leur utilisation :* les technologies anti-UAS sont loin d'être des

outils prêts à l'emploi. Avant de les déployer, il convient d'analyser avec précision si les systèmes sont conformes aux lois nationales et d'évaluer en détail les particularités du ou des sites où elles seront utilisées. De plus, elles peuvent être rapidement dépassées compte tenu du rythme auquel évoluent les technologies liées aux UAS. En outre, comme il s'agit de systèmes complexes, elles sont souvent coûteuses et requièrent une formation approfondie ainsi qu'une certaine connaissance de leurs caractéristiques pour pouvoir être utilisées en toute sécurité.

Par ailleurs, l'éventail de contre-mesures conçues particulièrement pour protéger les cibles vulnérables peut être considérablement limité. Par exemple, une technologie donnée peut représenter une solution efficace et raisonnable contre les UAS utilisés à des fins terroristes dans une zone reculée, mais se révéler totalement inadéquate pour protéger l'espace aérien au-dessus d'un aéroport ou un événement à forte affluence. De même, détruire un UAS survolant une zone urbaine densément peuplée ou faire perdre le contrôle de l'appareil peut entraîner l'écrasement de l'engin au sol et causer des blessures ou des dommages importants, notamment si le système est utilisé comme arme, provoquant une explosion incontrôlée. En outre, l'utilisation de mesures électroniques pour lutter contre les drones dans les environnements où l'activité électromagnétique est complexe, comme les zones urbaines, peut s'avérer limitée vu le risque d'interférence avec les radiofréquences dont dépendent des services légitimes.

- *Lassitude face aux UAS :* comme le souligne le Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, « [n]ombre d'incidents dus à des systèmes d'aéronefs non habités sont le fait d'usages négligents, irréfléchis ou imprudents sans visée terroriste. Avec le temps, le fait de faire face à une succession d'incidents mineurs impliquant des systèmes d'aéronefs non habités peut engendrer un sentiment de complaisance chez les autorités ou dans le public. Il peut



en découler chez les responsables et le public une tendance à négliger les vulnérabilités, les signes d'alerte précoce, les notifications publiques ou les menaces crédibles, ce qui accroît d'autant le niveau de vulnérabilité à une attaque réelle. » [Bonne pratique n° 5, Forum mondial de lutte contre le terrorisme (2019)].

Encadré 3.
Vulnérabilités dans l'infrastructure informatique des systèmes de drone aérien

L'infrastructure informatique mise en place par les fabricants de systèmes de drone aérien peut présenter un ensemble spécifique de vulnérabilités. Les possibilités d'intrusions hostiles peuvent être d'autant plus grandes lorsque les producteurs proposent des services basés sur un écosystème complexe composé de plusieurs éléments et d'applications tierces destinées à étendre la fonctionnalité de l'appareil de base.

En 2018, une importante entreprise de fabrication de systèmes de drone aérien a découvert une vulnérabilité dans son infrastructure infonuagique qui aurait pu permettre à des attaquants de prendre le contrôle des comptes des utilisateurs et d'accéder à des données privées, telles que des photos et des vidéos prises lors des vols de drone, des renseignements sur le compte personnel des utilisateurs et des journaux de vol comprenant des données de localisation. Après avoir découvert cette vulnérabilité, l'entreprise ne l'a pas seulement corrigée, mais a également revu son approche quant à la manière dont ses systèmes informatiques gèrent l'authentification des utilisateurs.

Source : www.wired.com/story/dji-drones-bugs-exposed-users-data.

[3]

Atténuation des risques et intervention : rôles des parties prenantes et bonnes pratiques

Le chapitre qui suit traite de la façon dont les différentes parties prenantes impliquées dans l'écosystème des systèmes de drone aérien (acteurs institutionnels et non institutionnels) peuvent contribuer à atténuer le risque d'attaques terroristes perpétrées au moyen de ces systèmes et faciliter la gestion des crises et le retour à la normale, notamment en établissant des partenariats public-privé. Il est essentiel, dans ce domaine, de créer des partenariats durables et étroits, compte tenu des caractéristiques propres aux activités de conception, de fabrication et de commercialisation des systèmes de drone aérien et des technologies de lutte contre ces systèmes, qui sont largement dominées par le secteur privé.

3.1 États Membres

3.1.1 Décideurs

Les organismes gouvernementaux ont le devoir de mettre en place un cadre général visant à faciliter la prévention et la gestion des incidents impliquant des UAS, un retour à la normale rapide et un soutien pour les sites et personnes affectés après de tels incidents.

Parallèlement, les organismes gouvernementaux doivent fournir un environnement de travail juridique, institutionnel et collaboratif permettant de tirer parti des technologies UAS en tant qu'outils de protection des sites vulnérables exposés aux attaques terroristes en général, tout en préservant les droits humains.

Dans la poursuite de ces objectifs généraux, il est essentiel que les acteurs gouvernementaux fassent participer les diverses parties prenantes de l'écosystème des UAS (communautés d'utilisateurs, fabricants et fournisseurs d'UAS, fournisseurs de solutions anti-UAS, établissements universitaires et de recherche, organisations de la société civile, activistes, etc.) à une ou plusieurs étapes du processus d'élaboration des politiques. Leur participation est essentielle pour garantir que les résultats en matière de réglementation : 1) tiennent compte des attentes d'une vaste clientèle d'utilisateurs finaux ainsi que des difficultés auxquelles ils sont confrontés; 2) reflètent les préoccupations du secteur; 3) intègrent les menaces (y compris les nouveaux dangers), les modes d'attaque et les scénarios pertinents identifiés par les établissements de recherche, les services de renseignement, etc.; 4) prennent en compte les préoccupations et les besoins de la société civile en ce qui a trait à l'utilisation des UAS pour protéger les cibles vulnérables.

Outil 3.
Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités – Forum mondial de lutte contre le terrorisme (2019)
(www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20FR.pdf?ver=2020-01-13-143548-203)

Les bonnes pratiques du Mémorandum de Berlin ont pour but de soutenir les gouvernements dans leurs efforts de recensement, de rédaction et de révision des politiques, pratiques, lignes directrices, règlements, programmes et méthodes destinés à lutter contre l'utilisation d'UAS à des fins terroristes. Ce Mémorandum résume les points importants et les connaissances présentés par les gouvernements, les agences chargées de l'application de la loi, les organisations multilatérales, le secteur privé et d'autres experts en la matière au cours de quatre ateliers régionaux tenus respectivement en Allemagne, en Jordanie, en République de Corée et aux Pays-Bas en 2018 et 2019.

Le Mémorandum de Berlin décrit 26 bonnes pratiques regroupées en 4 grands domaines :

- *Évaluation du risque, évaluation des points de vulnérabilité et sensibilisation :* dans leurs procédures systématiques d'évaluation du risque, les États devraient tenir compte de l'utilisation potentielle d'UAS à des fins terroristes afin d'identifier, en

(suite)

collaboration avec les parties prenantes compétentes, les points de vulnérabilité et les failles des systèmes de protection. Ils devraient envisager l'ensemble des manières dont les terroristes pourraient utiliser les UAS ainsi qu'anticiper les avancées technologiques et tout autre facteur susceptible d'avoir une incidence sur la menace afin de pouvoir répondre à chaque nouvelle utilisation;

- *Meilleur partage des informations, participation des acteurs concernés et sensibilisation du public :* le caractère multidimensionnel de l'utilisation d'UAS à des fins terroristes exige la concertation des États, des organisations intergouvernementales régionales et internationales, ainsi que des acteurs non conventionnels. Les efforts déployés au niveau national pour lutter contre la menace d'utilisation d'UAS à des fins terroristes devraient être complétés par des mesures appliquées à l'échelle régionale et internationale, suivant les cas. Les États devraient également promouvoir, auprès du grand public, l'utilisation responsable des UAS et l'encourager à intervenir convenablement lorsqu'ils sont utilisés de manière suspecte;
- *Mise en œuvre de politiques et de règlements, planification de la gestion des crises :* les États devraient mettre en place des politiques et des règlements clairs et exécutoires ayant pour but de réduire, voire d'éliminer, la prolifération et l'utilisation malveillante d'UAS par des terroristes ou d'autres acteurs malintentionnés; de faciliter la lutte efficace contre ces systèmes; et de permettre le bon déroulement et l'efficacité des enquêtes, poursuites et sanctions en lien avec les UAS. Les gouvernements devraient également élaborer des stratégies de gestion et d'atténuation de crise afin d'intervenir adéquatement après les incidents impliquant des UAS;
- *Élaboration de contre-mesures tactiques et de solutions techniques :* les États devraient mettre en place des mesures de protection et autres solutions techniques et les soumettre à un examen régulier. Pour ce faire, il faut équiper et former les autorités compétentes à reconnaître et contrer l'utilisation malintentionnée d'UAS. Avant de recourir à des contre-mesures, les États devraient en évaluer et atténuer les effets négatifs en coopération avec les parties concernées. Il faut aussi tenir compte de ce qu'elles mobilisent parfois des ressources considérables et entraînent des besoins importants en formation.

Outil 4.
Trousse d'outils de l'Organisation de l'aviation civile internationale (OACI) pour les UAS
(www.icao.int/safety/UA/UASToolkit/Pages/default.aspx)

Cette trousse d'outils est une initiative Web élaborée en coopération avec le secteur et le réseau d'experts internationaux partenaires de l'OACI. Elle regroupe des règlements et des pratiques exemplaires afin d'aider les États Membres à élaborer des orientations opérationnelles efficaces concernant l'utilisation des UAS. Elle permet d'accéder notamment aux règlements existants dans le monde, à des ressources liées aux questions techniques et opérationnelles (telles que la formation et l'éducation des exploitants d'UAS) et à des orientations pour les campagnes nationales de sensibilisation.

3.1.1.1 Stratégies de lutte contre les systèmes de drone aérien

La lutte contre la menace que représente l'utilisation des UAS à des fins terroristes est une responsabilité multipartite qui nécessite une coordination et une vision commune. Un des objectifs primordiaux des gouvernements consiste à lancer, diriger et soutenir cet effort de coordination en définissant clairement la vision et les approches globales qui devraient sous-tendre la position des pays dans la protection contre l'utilisation des UAS à des fins terroristes. Cela nécessite pardessus tout de déterminer les mécanismes que doivent utiliser les différents types de réglementation ou de contrôle des UAS pour se concerter et définir les modalités et les types de partenariats public-privé qui conviennent (plateformes d'échange d'informations avec le secteur, programmes de sensibilisation des exploitants de sites, etc.)[25].

La menace que posent les UAS utilisés à des fins terroristes peut être prise en compte et traitée dans des stratégies conçues spécialement à cette fin[26] ou encore dans des démarches plus générales visant à contrer le terrorisme ou à assurer la sécurité nationale, comme celles qui portent sur la protection des cibles vulnérables. S'il existe plusieurs documents ou cadres institutionnels, il est essentiel qu'ils soient cohérents en ce qui concerne la vision, les approches, les procédures et les attentes établies[27]. Enfin, certains pays peuvent choisir d'intégrer leur approche de prévention et de lutte contre les menaces que posent les UAS dans leur stratégie globale visant à encourager le développement

25 Les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité soulignent également la nécessité d'adopter une approche pangouvernementale et exhaustive pour lutter contre l'achat et l'utilisation d'UAS par des terroristes, et l'impératif d'assurer un contrôle régulier à l'aide d'un processus multipartite inclusif. Voir la section 2.1.1 du sous-module II sur les politiques et les stratégies nationales.

26 Le Royaume-Uni a suivi cette approche en élaborant une stratégie conçue spécialement pour lutter contre les UAS [Royaume-Uni (2019)].

27 Certains pays peuvent confier l'élaboration des stratégies de lutte contre les UAS à leurs ministères. Le Département de la défense des États-Unis, par exemple, a élaboré une stratégie spécialisée [États-Unis d'Amérique (2021)] après avoir constaté que les petits UAS faisaient peser sur son personnel, ses activités et ses installations des risques de plus en plus élevés – que cette menace provienne d'acteurs étatiques ou autres. Il est clair que ces stratégies d'envergure ministérielle doivent s'inscrire dans les démarches gouvernementales plus générales visant à gérer les menaces liées aux UAS.

d'économies sûres, porteuses de croissance et socialement utiles faisant usage d'UAS[28].

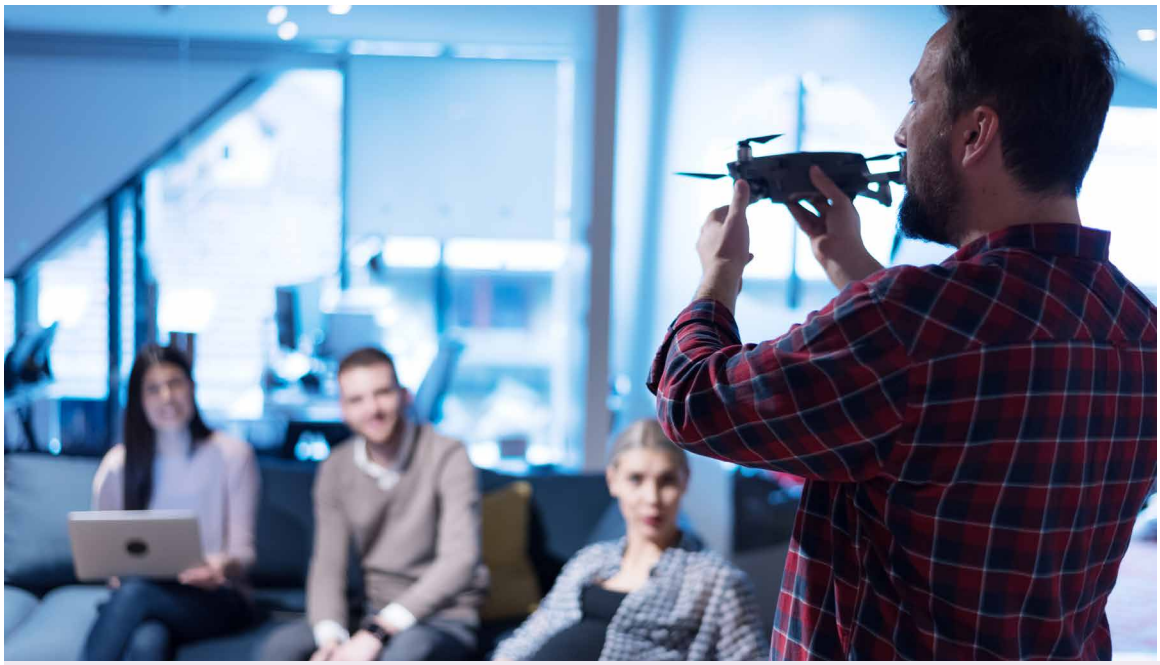
Sur le plan procédural, les pays qui entreprennent d'élaborer une stratégie de lutte contre les UAS devraient mener une consultation pangouvernementale qui permettra de produire un document stratégique ciblé et complet.

Les questions prioritaires qui doivent être abordées dans toute stratégie nationale comprennent notamment :

- *Les liens entre les secteurs civil et militaire :* le modèle de coordination interinstitutions repose notamment sur la collaboration entre les secteurs civil et militaire. À cet égard, le Mémorandum de Berlin encourage les pays à « prendre en considération l'expérience acquise et les enseignements tirés par les forces nationales de défense [dans la mesure où plusieurs] composantes des forces armées ont acquis de l'expérience dans la lutte contre l'utilisation de systèmes d'aéronefs non habités par des acteurs violents non étatiques dans le cadre de conflits armés[29] » [Bonne pratique nº 11, Forum mondial de lutte contre le terrorisme (2019)];
- *La coordination entre les autorités du secteur de l'aviation :* toute stratégie gouvernementale doit promouvoir des mécanismes permettant la communication étroite et l'échange d'informations entre les autorités de l'aviation civile, les fournisseurs de services de navigation aérienne et les organismes responsables de la sûreté et de la sécurité aériennes. À la base, l'interaction fonctionnelle entre ces organismes semble nécessaire pour que les cadres de réglementation des UAS soient pertinents et à jour. En outre, comme le précise le Mémorandum de Berlin, « [c]ompte tenu des effets imprévus que peuvent avoir les contre-mesures, en particulier au regard de la sécurité de l'aviation civile et des systèmes (de communication) par radiofréquences », les autorités de l'aviation civile et les fournisseurs de services de navigation aérienne peuvent « aider à atténuer autant que possible les conséquences indésirables des contre-mesures » [Bonne pratique nº 13, Forum mondial de lutte contre le terrorisme (2019)]. En outre, « au vu de l'éclairage utile et précoce que ces entités peuvent apporter concernant les effets des contre-mesures envisagées sur la sécurité et sur les opérations aériennes », leur collaboration est souhaitée;
- *La participation des exploitants de cibles vulnérables :* les gouvernements doivent déterminer le type d'initiatives et de programmes publics à mettre en place pour aider les exploitants de sites à accroître leur résilience face aux attaques terroristes impliquant des UAS. En fonction des ressources budgétaires disponibles, les mesures incitatives peuvent prendre diverses formes (subventions, plans de financement, allègements fiscaux, etc.). Les gouvernements peuvent également soutenir les exploitants de sites en leur donnant accès à de l'expertise, comme des conseils spécialisés sur la gestion des risques et des crises offerts par des unités compétentes en matière de maintien de l'ordre ou de sécurité nationale.

28 La stratégie de Transports Canada en matière de drones, par exemple, comporte un volet consacré expressément à la sécurité. Adoptée en 2021, elle décrit la vision stratégique du Canada en ce qui concerne les UAS et vise avant tout à mieux faire connaître l'importance des UAS et à définir les priorités politiques à respecter d'ici 2025 [Canada (2021)].

29 Le Mémorandum de Berlin précise toutefois que « les enseignements tirés des théâtres des conflits ne sont pas toujours transposables aux stratégies de lutte contre les systèmes d'aéronefs non habités élaborées pour une configuration nationale en dehors du contexte d'un conflit armé ». En effet, comme bon nombre de systèmes ont été conçus pour être utilisés sur le champ de bataille, ils ne représentent pas une solution viable dans l'espace aérien intérieur qui surplombe les zones habitées.



Encadré 4.
Stratégie pangouvernementale recommandée par l'OACI pour les systèmes de drone aérien

Compte tenu de la complexité du sujet et du grand nombre d'organismes gouvernementaux concernés, la trousse d'outils de l'OACI recommande aux États d'adopter une stratégie pangouvernementale en ce qui concerne les UAS, qui pourrait comprendre des composantes clés comme :

- Une feuille de route qui définit les objectifs économiques et en matière de sécurité et de sûreté de l'industrie future des UAS;
- Un comité interdépartemental du gouvernement sur les UAS chargé de partager les informations et d'aider les départements exploitant des UAS à planifier leurs activités;
- Une méthodologie d'alignement des besoins de l'industrie sur les ressources publiques;
- Des activités de coordination visant à élargir l'accès des parties prenantes de l'industrie aux financements nécessaires pour étudier de nouvelles technologies et commercialiser des applications.

Source : www.icao.int/safety/UA/UASToolkit/Pages/default.aspx.

En outre, les États qui s'efforcent de protéger les infrastructures de l'aviation civile contre les actes d'intervention illicite perpétrés au moyen de drones aériens devraient également prendre en considération les mesures décrites à ce sujet au chapitre 19 du Manuel de sûreté de l'aviation de l'OACI (Doc 8973, diffusion restreinte).

Étude de cas 1.
Stratégie de l'Union européenne pour lutter contre les systèmes de drone aérien en contexte antiterroriste

L'approche actuelle de l'Union européenne est structurée sous forme d'un vaste projet interinstitutionnel et intersectoriel qui tire parti du travail de divers organes de l'Union européenne, des réseaux de défense et de maintien de l'ordre, et de consortiums financés. Les activités et initiatives réalisées ont mené à l'établissement d'un cadre juridique, politique et institutionnel qui évolue rapidement et dont les principales composantes sont les suivantes :

- La Stratégie de l'Union européenne pour l'union de la sécurité et la version mise à jour du Programme de lutte antiterroriste (2020);
- Le cadre réglementaire de l'Union européenne applicable aux exploitations sécuritaires de drones, prévu dans les règlements 2019/945 et 2019/947;
- Les travaux en cours visant la création des services « U-space » aux fins de la gestion du trafic d'aéronefs sans équipage à bord (système de gestion du trafic de l'UE);
- Le Plan d'action sur les synergies entre les industries civile, spatiale et de la défense (2021);
- Les initiatives menées par le Centre commun de recherche de la Commission européenne sur la protection physique contre les UAS, y compris la protection des infrastructures critiques;
- Le manuel de l'UE sur la protection des zones urbaines contre les UAS non coopératifs, qui fait actuellement l'objet de consultations ciblées et devait être publié vers la fin de 2021.

Source : Réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (29 juin 2021).

Étude de cas 2.
UK Counter-Unmanned Aircraft Strategy
(Stratégie du Royaume-Uni pour lutter contre les drones aériens)

Conceptualisée sous forme d'un document prospectif, cette stratégie est censée évoluer au même rythme que la technologie afin de garder une longueur d'avance sur la menace posée par les UAS. Le Gouvernement britannique y présente les mesures envisagées pour lutter contre l'utilisation malveillante de petits UAS[30] et réduire le risque posé par les activités illégales les plus préjudiciables en s'appuyant sur quatre résultats stratégiques :

1. Acquérir une compréhension globale des risques posés par l'utilisation malveillante et illégale des UAS, risques qui sont en constante évolution;
2. Adopter une approche exhaustive pour empêcher, détecter et interrompre toute utilisation malveillante des UAS;
3. Établir des relations solides avec le secteur pour s'assurer que les produits offerts répondent aux normes de sécurité les plus élevées;
4. Renforcer les capacités des services de police et des autres intervenants opérationnels en leur donnant accès à des moyens de lutter contre les drones, ainsi qu'à des lois, de la formation et des conseils efficaces.

Cette stratégie a été élaborée pour compléter CONTEST, la stratégie britannique antiterroriste, ainsi que la stratégie de lutte contre les crimes graves et la criminalité organisée du pays.

Source : Royaume-Uni (2019).

30 L'Administration de l'aviation civile du Royaume-Uni définit les « petits UAS » comme ceux pesant moins de 20 kg. Les rédacteurs ont décidé de limiter l'application de la stratégie à ces systèmes, qui sont beaucoup plus accessibles et faciles à exploiter que les systèmes plus lourds.

Étude de cas 3.
L'approche de Singapour face aux risques de sécurité posés par les systèmes de drone aérien

Bien que Singapour n'ait subi aucune attaque directe de drones, le pays comprend que les intrusions d'UAS peuvent tout de même présenter d'autres risques, notamment pour la sécurité lorsque ces systèmes sont déployés dans le cadre de grands événements de forte affluence. En outre, en juin 2019, la présence d'UAS autour de l'aéroport de Changi a contraint les autorités à restreindre temporairement les opérations sur les pistes, ce qui a entraîné des retards et le déroutement de certains vols.

L'approche globale de Singapour, qui vise à assurer un équilibre entre les risques de sécurité/sûreté et les utilisations légitimes des UAS, repose sur trois piliers :

- **Réglementation :** le Parlement de Singapour a adopté un projet de loi sur les drones aériens (sûreté et sécurité publiques) en 2015 afin de réglementer l'exploitation des drones, et un projet de loi sur la navigation aérienne (modification) en 2019 en vue de renforcer les mesures de contrôle à l'égard de ces appareils. Ces textes législatifs s'appuient sur trois principes de base : 1) certains vols de drones nécessitent un permis (notamment ceux effectués à une distance de 5 kilomètres ou moins d'un aérodrome civil ou militaire, dans une zone protégée, restreinte ou dangereuse, ou à plus de 200 pieds (environ 60 mètres au-dessus du niveau de la mer); 2) les activités dangereuses réalisées à l'aide de drones sont interdites (par exemple, tout largage à partir d'un UAS); 3) les UAS pesant plus de 250 grammes doivent être enregistrés;

  Les sanctions applicables sont proportionnelles aux conséquences de l'exploitation illégale des UAS (par exemple, survoler une zone protégée sans permis peut donner lieu, lors d'une première infraction, à diverses sanctions, dont une amende pouvant aller jusqu'à 50 000 dollars et une peine d'emprisonnement d'une durée maximale de deux ans);
- **Maintien de l'ordre :** les autorités interviennent, enquêtent et engagent des poursuites dans les cas de non-respect de la réglementation;
- **Sensibilisation :** de solides politiques de sensibilisation du public sont mises en œuvre afin de promouvoir l'utilisation responsable des UAS et de faire mieux connaître la réglementation.

Source : Intervention de M. Lee Peng Yang, Directeur adjoint principal du Groupe mixte des opérations du Ministère de l'intérieur de Singapour, à la réunion du Groupe d'experts du Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

3.1.1.2 Cadres juridiques généraux relatifs aux systèmes de drone aérien

Bien que les pays adoptent diverses approches réglementaires pour régir l'exploitation des UAS sur leur territoire, la plupart jugent prioritaire le « principe de la sécurité d'abord », qui se traduit généralement par une série d'exigences telles que l'octroi de licences de pilote, l'immatriculation des aéronefs, la souscription d'assurances et la création de zones d'exclusion aérienne (habituellement aux abords des infrastructures critiques). Bien que de nombreux pays n'imposent ces exigences qu'aux UAS commerciaux, certains d'entre eux ont récemment étendu les systèmes d'enregistrement obligatoires aux petits UAS utilisés à des fins récréatives[31].

Lors de l'élaboration des différents segments de leurs cadres réglementaires, l'OACI recommande aux États de « consulter les parties prenantes clés au début du processus d'élaboration des règlements. Il pourrait se révéler efficace de créer un groupe de travail conjoint gouvernement/parties prenantes chargé de passer en revue la législation existante et de formuler des recommandations pour un nouveau cadre réglementaire des UAS. Parmi les parties prenantes des UAS devraient figurer les exploitants, les constructeurs et les organisations d'aéronefs habités. Une fois les règlements élaborés, le fait de solliciter des commentaires de parties prenantes tant aéronautiques qu'extra-aéronautiques permettra d'assurer la prise en compte de toutes les exigences pertinentes par les règlements. »[32] En outre, il est fondamental que la législation relative aux drones évolue au même rythme que la menace, tienne compte de l'expérience opérationnelle et éclaire indirectement la formation et l'orientation données[33].

31 Les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité mentionnent la nécessité de mettre en place des cadres législatifs et réglementaires adéquats pour prévenir et réduire les menaces posées par l'acquisition ou l'utilisation d'UAS à des fins terroristes, et décrit certaines difficultés rencontrées à cet égard. Voir sous-module II, section 2.1.3 sur la législation et la réglementation internes.

32 Trousse d'outils de l'OACI, Autres considérations (www.icao.int/safety/UA/UASToolkit/Pages/default.aspx).

33 Voir https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf.

Encadré 5.
Gestion du trafic des systèmes de drone aérien

Les systèmes de gestion du trafic aérien existants ne sont pas adaptés pour faire face à l'augmentation du trafic généré par les UAS de toutes sortes et pour encadrer leurs profils de vol. C'est pourquoi il sera important de créer des systèmes de gestion du trafic des UAS pour contrôler la circulation de ces appareils à basse altitude, définir l'espace aérien réglementé et accorder ou refuser ponctuellement l'accès aux zones contrôlées[34].

La conception et le déploiement sûrs de systèmes de gestion du trafic des UAS peuvent également aider les autorités à distinguer les appareils exploités en toute légalité de ceux susceptibles d'être utilisés illégalement ou à des fins malveillantes. De tels systèmes pourraient fournir des renseignements clés lors des interventions réalisées en cas d'incident[35].

Cependant, de plus en plus de pays mettent en place des cadres réglementaires et opérationnels sans se concerter, ce qui risque de créer des problèmes de compatibilité et de coordination entre les divers systèmes de gestion du trafic des UAS. Il est également possible que des renseignements de nature délicate concernant des civils ou des gouvernements soient transmis de manière non sécurisée en raison de l'incompatibilité des systèmes de gestion utilisés. En outre, les technologies de détection des UAS (voir section 3.1.2.2) seront tout de même nécessaires à des endroits et lors d'événements particuliers pour composer avec les appareils non conformes. Les questions de compatibilité entre les technologies de détection et les systèmes de gestion du trafic des UAS pourraient donc devenir d'autant plus importantes dans l'avenir.

34 Les systèmes de gestion du trafic des UAS peuvent être fixes ou mobiles selon leur utilisation. Les systèmes fixes permettraient de couvrir en tout temps des zones particulières, telles que l'espace aérien inférieur encombré au-dessus des grandes zones urbaines. Les systèmes mobiles pourraient plus facilement être transportés lors d'événements particuliers (rassemblement de masse, sinistre, etc.).

35 L'OACI a élaboré à cette fin un document d'orientation sur la gestion du trafic des UAS, qui peut être consulté à l'adresse www.icao.int/safety/UA/Pages/UTM-Guidance.aspx.

Étude de cas 4.
Cadre de réglementation des systèmes de drone aérien de l'Union européenne

En 2019, l'Union européenne a introduit un cadre réglementaire visant à tirer parti des retombées économiques et sociales des UAS tout en soumettant les fabricants et les exploitants à une série de restrictions ayant pour but d'assurer la sûreté et la sécurité publique, la protection des données personnelles, le respect de la vie privée ainsi que la protection de l'environnement, y compris en limitant la pollution sonore. Les règlements 2019/947 et 2019/945 de l'UE, dont l'approche repose sur les risques, ne font pas de distinction entre les activités commerciales et récréatives; ils tiennent plutôt compte du poids de l'appareil et de l'utilisation qui en sera faite. Selon ce concept, les utilisations sont classées dans les catégories « ouverte », « spécifique » ou « certifiée », en fonction du niveau de risque évalué :

- Catégorie ouverte : cette catégorie comprend les utilisations présentant les risques les plus faibles. Aucune autorisation n'est requise avant le vol.
- Catégorie spécifique : une autorisation d'exploitation délivrée par l'autorité nationale compétente est requise. Pour ce faire, il faut procéder à une évaluation des risques de sécurité, qui déterminera les exigences à respecter pour que l'exploitation ne pose pas de risque.
- Catégorie certifiée : le risque de sécurité est considéré comme très élevé et nécessite la certification du drone et de l'exploitant ainsi que l'octroi d'une licence au(x) pilote(s) à distance.

Source : Règlements 2019/947 et 2019/945 de l'UE.

Étude de cas 5.

Cadre de gestion des risques des Émirats arabes unis concernant les aéronefs non autorisés dans l'espace aérien contrôlé

En novembre 2016, l'Autorité de l'aviation civile des Émirats arabes unis a introduit des mesures d'urgence visant les aéronefs non autorisés dans l'espace aérien contrôlé (décision de sécurité nº 2016-16). La réglementation fournit des orientations à l'intention des fournisseurs de services de navigation aérienne sur l'évaluation tactique des risques liés aux intrusions dans l'espace aérien contrôlé, ainsi que sur les mesures d'atténuation à prendre tout en veillant à adapter lesdites mesures au risque posé par l'intrus.

Le cadre repose sur les procédures conceptuelles suivantes :

- L'établissement, la mise en œuvre et le maintien d'un système de gestion de la sécurité par les organismes des services de la circulation aérienne;
- L'évaluation tactique des risques afin de déterminer les mesures qu'il convient de prendre en cas de violation de l'espace aérien.

Le texte intégral de la décision de sécurité nº 2016-16 a été présenté par les Émirats arabes unis lors de la treizième Conférence de navigation aérienne de l'OACI. La version anglaise de la décision peut être consultée à l'adresse www.icao.int/Meetings/anconf13/Documents/WP/wp_097_fr.pdf.

Outil 5.
Model UAS Regulations (modèle de réglementation des UAS) – OACI
(www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx)

Le modèle de réglementation de l'OACI est conçu pour aider les pays à établir et à mettre au point leurs lignes directrices nationales en ce qui concerne l'exploitation interne des UAS. Il découle d'une évaluation de l'OACI portant sur les règlements existants afin d'en extraire les points communs et les pratiques exemplaires conformes à son cadre d'aviation.

Il peut être téléchargé sur le site Web de l'OACI et devrait être régulièrement mis à jour pour suivre l'évolution et l'expansion des programmes nationaux sur les UAS. Les pays peuvent choisir d'adopter le règlement proposé dans son intégralité ou sélectionner certaines dispositions pour compléter les cadres nationaux existants. Cette réglementation moderne couvre les aspects essentiels de la certification et de l'exploitation sécuritaire des UAS dont les pays ont besoin.

3.1.1.3 Soutenir la conception et l'utilisation proportionnelle des technologies de lutte contre les systèmes de drone aérien

Les gouvernements ont la responsabilité de créer un environnement favorable à la conception et à l'utilisation appropriée de technologies anti-UAS, notamment dans le but de protéger les sites vulnérables contre les activités terroristes impliquant des UAS[36]. Du point de vue de l'élaboration des politiques en général, au moins trois groupes de questions doivent être pris en considération :

- Il convient de déterminer quels organismes gouvernementaux et services de maintien de l'ordre ont pour mission de mener des opérations anti-UAS et sur quelles protections et exigences légales ils s'appuient pour ce faire[37]. Les gouvernements qui accordent des pouvoirs à certaines autorités nationales pour lutter contre les UAS doivent déterminer les modalités à respecter pour garantir que ces technologies seront utilisées de manière proportionnelle et dans le respect des droits humains. Les règlements pertinents devraient, par exemple, intégrer les

36 Les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité donnent une vue d'ensemble des technologies anti-UAS, y compris des difficultés et des préoccupations qu'elles soulèvent. Voir sous-module II, section 3.1 sur les systèmes et les techniques de lutte contre les UAS, section 2.2 sur le développement de capacités, de normes et d'opérations pour lutter contre les UAS, et section 3.8 sur l'élaboration de contre-mesures liées aux UAS.

37 Actuellement, les pays n'abordent pas tous cette question de la même manière. Alors que certains cadres juridiques définissent qui a la responsabilité de lutter contre les UAS – parfois de manière fragmentée et complexe –, d'autres ne contiennent aucune disposition précise à ce sujet.

normes de base à respecter en matière de preuve et de procédure, comme la nécessité de démontrer la cause probable ou toute exigence équivalente, avant que les forces de l'ordre soient autorisées à agir contre des UAS menaçants. Les politiques anti-UAS peuvent également tenir compte de la mesure dans laquelle les interventions des forces de l'ordre doivent être précédées d'une notification ou d'un avertissement laissant à l'exploitant une possibilité raisonnable de prendre des mesures correctives (changer la direction de l'appareil, atterrir en dehors du périmètre de sécurité, etc.);

- Comme les technologies anti-UAS ne sont souvent pas des outils prêts à l'emploi et nécessitent l'acquisition d'importantes compétences techniques ainsi qu'une formation connexe, leur achat et leur utilisation par les organismes compétents pourraient être régis par des cadres réglementaires exigeant la réussite de tests appropriés en vue de garantir une utilisation habile et sûre;
- Il convient de déterminer comment les organismes gouvernementaux communiqueront avec les parties prenantes du secteur chargées de concevoir les technologies anti-UAS. Cette concertation étendue doit avoir au moins pour objectif de garantir que les technologies intégrées au bout du compte dans les dispositifs de lutte contre les UAS respectent les spécifications et contraintes réglementaires. Les gouvernements devraient également établir leurs politiques de financement (en fonction des ressources budgétaires disponibles, des règles de concurrence en vigueur, etc.) en vue de soutenir les innovations scientifiques et techniques dans le secteur des technologies anti-UAS et envisager, notamment, d'aider les petites et les jeunes entreprises à proposer des solutions novatrices[38].

Étude de cas 6.
Projet Courageous : méthodologie permettant de choisir la bonne technologie pour lutter contre les systèmes de drone aérien

Mis en œuvre par le laboratoire de recherche en robotique et systèmes autonomes (Robotics & Autonomous Systems) de l'École royale militaire de Belgique[39], le projet Courageous repose sur le constat que comme les UAS « sont de plus en plus accessibles, les forces de l'ordre se retrouvent maintenant avec l'obligation d'assurer le maintien de l'ordre dans l'espace aérien inférieur. Les fournisseurs commerciaux ont déjà conçu un large éventail de solutions à cette fin, mais les capacités des systèmes élaborés sont difficiles à comparer. Les utilisateurs finaux ont donc du mal à déterminer quels outils conviennent à leur contexte ». En 2019, par exemple, il existait plus de 100 systèmes

38 La stratégie du Royaume-Uni pour lutter contre les drones aériens, par exemple, envisage l'établissement de partenariats solides avec les entreprises de technologies anti-UAS dans le but, notamment, de recenser les capacités approuvées de lutte anti-drones dans un seul document gouvernemental. Ce catalogue national serait ensuite mis à la disposition des partenaires pour les aider à faire des achats éclairés (UK Counter-Unmanned Aircraft Strategy, p. 24).

39 Avec le soutien de la Commission européenne.

commerciaux anti-UAS; or, dans bien des cas, aucune preuve n'étayait l'efficacité alléguée, et les différentes méthodes d'essai utilisées rendaient très difficiles les comparaisons.

Le projet Courageous pallie ces difficultés grâce à une méthodologie normalisée pour la mise à l'essai des systèmes de détection, de suivi et d'identification des UAS. Cette méthodologie est fondée sur une série de scénarios standard définis par les utilisateurs (sécurité dans les prisons et les aéroports, protection des infrastructures critiques, sécurité des frontières, commerce de la drogue, traite des personnes, etc.). Pour chacun de ces scénarios, les utilisateurs finaux du projet Courageous établissent les besoins opérationnels et les exigences techniques et fonctionnelles. Sur la base de ces informations, une méthode d'essai intégrale sera mise au point afin de permettre une comparaison qualitative et quantitative des différents systèmes anti-UAS. Cette méthode d'essai sera validée au cours de trois exercices préparés par les utilisateurs.

Sources : https://mecatron.rma.ac.be/index.php/projects/isf-courageous/; et intervention de Geert De Cubber de l'École royale militaire de Belgique lors de la réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

Étude de cas 7.
Programme de financement de l'accélérateur de défense et de sécurité (Defence and Security Accelerator) – Royaume-Uni

En 2020, un concours a été lancé dans le cadre de l'accélérateur de défense et de sécurité (une initiative intergouvernementale du Ministère de la défense du Royaume-Uni) pour le financement de propositions visant l'élaboration de technologies anti-UAS et décrivant comment intégrer ces technologies pour créer un système efficace. Toutes les propositions devaient expliquer comment les technologies présentées pouvaient être développées pour établir un système opérationnel contre les menaces posées par les petits UAS commerciaux, improvisés ou militaires. Elles devaient également démontrer :

- une approche de conception novatrice;
- une nette amélioration par rapport aux solutions anti-UAS existantes;
- la façon d'incorporer les technologies dans des solutions;
- la manière d'exploiter le système ainsi créé.

Source : www.gov.uk/government/organisations/defence-and-security-accelerator.

3.1.1.4 Éducation et sensibilisation

Les utilisateurs finaux d'UAS, en particulier de drones de loisir, sont nombreux à ne pas suivre l'évolution des lois applicables et à ne pas respecter les normes de sécurité. Les autorités gouvernementales ont donc un rôle important à jouer en vulgarisant les cadres de réglementation en matière de sûreté et de sécurité qui s'avèrent, dans bien des cas, complexes et très techniques.

Tout programme de sensibilisation doit tenir compte de l'hétérogénéité des utilisateurs d'UAS en ce qui concerne l'âge, le genre, le niveau d'éducation et les motivations. Il existe divers moyens et techniques pour communiquer les renseignements clés, notamment les plateformes en ligne des vendeurs, les médias sociaux, les brochures que les fabricants distribuent avec les appareils et les manuels d'utilisation, les formations obligatoires ou facultatives et les activités de sensibilisation destinées aux exploitants[40].

Étude de cas 8.
Portail de ressources « Sécurité des drones »

Le portail de ressources « Sécurité des drones » est géré par le gouvernement du Canada. Il fournit du matériel informatif et éducatif à l'intention des exploitants de drones et décrit aussi bien les étapes nécessaires à l'immatriculation d'un drone qu'à l'obtention d'une licence de pilote. Un formulaire en ligne permet aux utilisateurs de signaler les incidents.

Source : https://tc.canada.ca/fr/aviation/securite-drones.

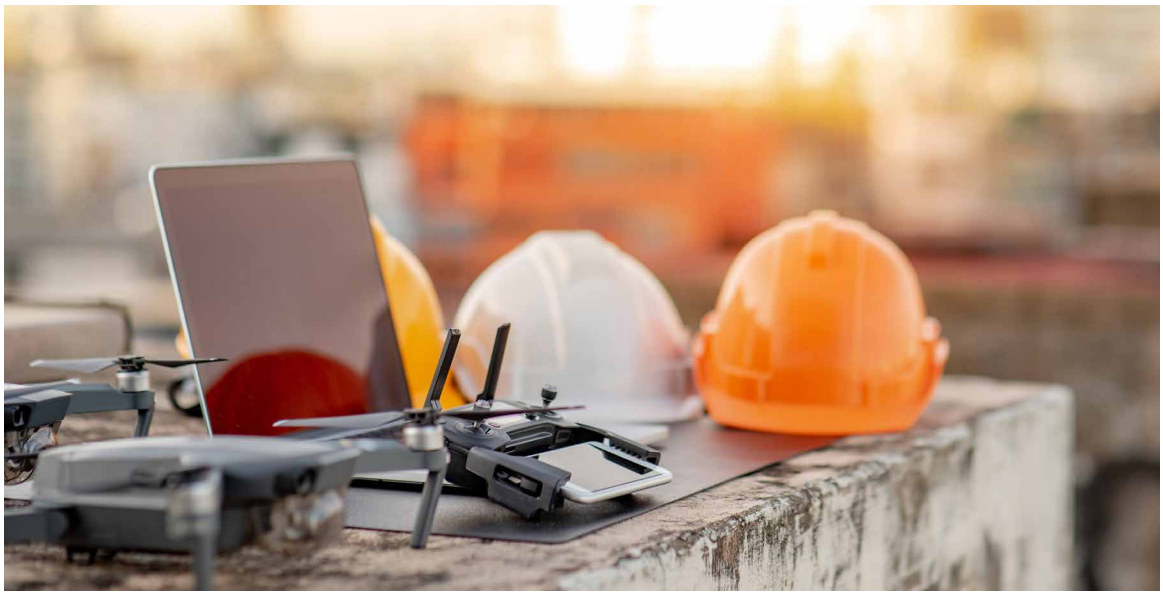
40 Les gouvernements peuvent également envisager d'utiliser les médias et les publications consacrées aux drones afin de sensibiliser les utilisateurs aux questions de sécurité, comme le prévoit la stratégie du Royaume-Uni pour lutter contre les drones aériens. Cette même stratégie prévoit également d'encourager le public à signaler les utilisations malveillantes de drones et de mener de vastes campagnes appelant à la vigilance à l'égard de toute utilisation suspecte, au même titre que toute autre activité terroriste ou criminelle. En faisant mieux connaître les conséquences juridiques possibles, nous donnerons plus de force à notre discours et les contrevenants ne pourront plus feindre l'ignorance [Royaume-Uni (2019), p. 21].

Outil 6.
Communication avec l'extérieur : information et sensibilisation – trousse d'outils de l'OACI pour les UAS
(www.icao.int/safety/UA/UASToolkit/Pages/Narrative-Considerations_fr.aspx)

Pour assurer le succès de l'intégration des UAS dans le système actuel des aéronefs habités, il est essentiel que les pilotes, les exploitants, les constructeurs, les acheteurs, les vendeurs, les importateurs et le grand public soient tous conscients des UAS. Fait plus important, le télépilote doit accepter la responsabilité et comprendre qu'il lui incombe d'assurer une exploitation en toute sécurité des UAS et d'en rendre compte. Des slogans comme « VOUS êtes maintenant un TÉLÉPILOTE » ou « VOUS êtes en position de CONTRÔLE » peuvent être intégrés dans les campagnes de sensibilisation. Le message devrait aussi inclure un rappel du risque de sécurité que pourraient poser les vols des UAS à proximité d'un aéroport ou d'un aéronef.

Information :
Les constructeurs, importateurs et vendeurs d'UAS doivent être formés à transmettre les renseignements de sécurité essentiels directement aux acheteurs. L'information peut être transmise des manières suivantes :

- Référence en ligne à la réglementation ou aux orientations particulières de l'État concernant les UAS – les hyperliens doivent être facilement accessibles;
- Document simple, clair et disponible en ligne sur les choses à faire et à ne pas faire lors de l'exploitation d'un UAS;
- Brochures ou matériel éducatif sur la réglementation et les orientations à l'intention des constructeurs, des vendeurs et des acheteurs d'UAS, des forces de l'ordre et des établissements universitaires.



(suite)

Campagnes de sécurité :

Il peut se révéler efficace de mettre en place des kiosques d'information lors des conférences, des salons aéronautiques et des foires commerciales. Il convient de songer à utiliser des événements existants comme forums de sensibilisation aux UAS. D'autres entités qui pourraient jouer un rôle dans la fourniture d'informations et la sensibilisation sont énumérées ci-dessous. Le recours aux services de ces entités peut permettre de diffuser les informations à l'échelle mondiale.

- Les bureaux d'immigration, notamment les services de conseil aux voyageurs;
- Les bureaux de tourisme;
- Les médias sociaux, notamment des pages Web mises à jour fréquemment comme YouTube et les blogues;
- Les sites Web et un manuel expliquant la réglementation, les dépliants et les campagnes de communication médiatique peuvent aussi être utilisés pour informer le grand public et les exploitants d'UAS;
- Les exploitants immatriculés peuvent aussi être informés par courrier électronique si l'autorité de l'aviation civile établit des listes de diffusion;
- Il peut être utile de créer une page consacrée aux questions fréquemment posées, notamment un processus de réponse aux questions par courrier électronique;
- Des outils en ligne facilitant l'appréciation de la situation et la planification de vol;
- Les campagnes de sécurité organisées par l'autorité de régulation dans le cadre du programme de sécurité/des activités de sensibilisation à l'aviation de son État.

3.1.1.5 Collaboration intergouvernementale

Toute politique nationale globale visant à lutter contre l'utilisation d'UAS à des fins terroristes devrait être établie après avoir considéré :

- Comment cette politique nationale peut tirer parti des enseignements et des expériences d'autres pays, notamment en ce qui concerne la promotion et la protection des droits humains et des libertés fondamentales;
- Comment reprendre à plus grande échelle les succès locaux de gestion et d'atténuation des risques et des crises en lien avec les UAS;
- Comment soutenir les enquêtes et les procédures pénales qui se déroulent dans d'autres pays en lien avec la préparation ou la perpétration d'actes terroristes impliquant des UAS qui comportent des éléments transnationaux;
- Comment s'assurer que la politique nationale est conforme à l'état de droit et respecte les droits humains.

Les objectifs ci-dessus exigent une coopération internationale proactive et des forums et des accords bilatéraux, régionaux ou multilatéraux. Les aspects à l'égard desquels les pays peuvent collaborer sont particulièrement nombreux[41] et comprennent notamment :

41 Voir sous-module II, section 2.5 des directives techniques pour l'application de la résolution 2370 du Conseil de sécurité portant sur la coopération internationale et régionale et l'échange d'informations.

- L'harmonisation des définitions et des classifications des UAS, des incidents connexes et des normes qui régissent la mise à l'essai des contre-mesures : l'établissement d'une base terminologique et de normes de travail communes sera essentiel à la compilation de statistiques pertinentes à l'échelle internationale et, par conséquent, aux comparaisons entre pays (en ce qui concerne l'évaluation des niveaux de menace, l'efficacité des contre-mesures, la présence de lacunes dans les pratiques et les politiques, etc.) [Bonne pratique n° 8, Forum mondial de lutte contre le terrorisme (2019)];
- La mise en place de mécanismes permettant aux autorités nationales de l'aviation de mettre leurs expériences en commun pour harmoniser leurs réglementations, en particulier lorsque les pays sont voisins;
- L'établissement éventuel d'une classification douanière particulière pour les UAS, dans le cadre d'initiatives multilatérales menées par l'Organisation mondiale des douanes, afin d'améliorer la capacité à détecter les envois suspects d'UAS[42];
- Comme le souligne l'OACI dans sa trousse d'outils pour les UAS, le lancement ou le renforcement d'initiatives de collaboration dans les domaines suivants :
  - Les exigences techniques, opérationnelles et de sécurité pour une exploitation en toute sécurité des UAS;
  - La recherche-développement, notamment le partage des résultats et l'identification de possibilités de collaboration sur des projets futurs et en particulier, la gestion de la circulation;
  - Les systèmes d'information;
  - Les stratégies de mise en application de la loi et de conformité à celle-ci, notamment les partenariats avec les organismes répressifs;
  - Les programmes de formation du personnel étatique chargé de la supervision des UAS.

42 Vu l'absence d'une norme de classification douanière propre aux UAS, les fabricants d'UAS légitimes utilisent les nomenclatures existantes (celle des caméras numériques, par exemple) pour décrire ce qu'ils expédient par les routes internationales.

- Le recours à des accords bilatéraux ou régionaux et à des plateformes multilatérales pour accroître l'échange d'informations entre les services de maintien de l'ordre au sujet des menaces, des modes opératoires, de l'identité, de la localisation et des activités des suspects, etc.;
- L'établissement de fondements et de mécanismes juridiques (dans des lois internes sur l'extradition et l'assistance judiciaire et des traités et instruments en matière de justice pénale) qui faciliteront l'échange d'éléments de preuve et l'extradition des fugitifs dans le cadre des procédures pénales intentées en lien avec des attaques terroristes impliquant des UAS ou leur préparation.

Encadré 6.
Difficultés en vue pour la coopération internationale dans la lutte contre les systèmes de drone aérien utilisés à des fins terroristes

Avec l'avènement de l'Internet des objets et de la technologie 5G, l'exploitation d'UAS à partir du Web, sans aucune proximité physique nécessaire entre l'aéronef et son pilote, pourrait bientôt devenir monnaie courante [Palestini (2020)]. Cette situation risque d'entraîner une augmentation du nombre de pays impliqués dans un même incident dû à des UAS et d'avoir des répercussions importantes sur la capacité de coopération pour l'application de la loi et les affaires judiciaires. Le pays à partir duquel un drone est exploité, par exemple, pourrait avoir à traiter rapidement une demande émanant du pays où le drone représente une menace afin d'identifier le pilote et de le mettre hors d'état de nuire. Certaines des mesures requises actuellement pour permettre aux gouvernements de coopérer efficacement contre la cybercriminalité pourraient bientôt devenir des outils essentiels pour endiguer les activités hostiles de drones.

3.1.1.6 Utilisation des systèmes de drone aérien pour protéger les cibles vulnérables

Les technologies qui sous-tendent l'utilisation des UAS à des fins terroristes peuvent également être employées par les autorités publiques et les exploitants de sites pour réaliser plus facilement d'importants objectifs de gestion des risques et des crises. Les utilisations qui peuvent être faites des UAS en tant qu'outils de protection des cibles vulnérables contre les attaques terroristes (menées ou non à l'aide d'UAS) sont nombreuses, et les décideurs devraient encourager le recours proactif aux UAS à cette fin. Les utilisations les plus pertinentes et les plus directes d'UAS pour la protection des cibles vulnérables dans les zones exemptes de conflits sont les suivantes :

- Repérer les vulnérabilités qui ne seraient pas autrement visibles ou facilement perceptibles depuis le sol, en particulier celles des grands sites (faiblesses dans le mur d'enceinte, zones vulnérables non suffisamment protégées contre d'éventuelles attaques aériennes, etc.);
- Faciliter la gestion des foules, notamment lors de grands concerts ou de grandes manifestations sportives, en alertant le personnel de sécurité, entre autres, de la présence d'un trop grand nombre de visiteurs dans certaines zones;
- Soutenir les efforts de gestion des crises pendant ou immédiatement après un attentat terroriste. Par exemple, les UAS peuvent faciliter les procédures d'évacuation des victimes, fournir des informations en temps réel sur l'étendue de la zone

touchée ainsi que sur la nature et l'ampleur des dégâts et aider les premiers secours à intervenir plus rapidement et plus efficacement auprès des victimes (en détectant les goulets d'étranglement et les embouteillages dans les zones avoisinantes, par exemple). En outre, les UAS équipés de caméras thermiques peuvent être utilisés de jour comme de nuit, dans le cadre des opérations de recherche et de sauvetage, pour repérer des signaux de chaleur;

- Soutenir les efforts communautaires de relèvement en facilitant, par exemple, la distribution de nourriture ou le transfert sûr de fournitures médicales difficilement acheminables par les moyens de transport traditionnels;
- Recueillir des renseignements dans le but, notamment, d'identifier ou de dénombrer les personnes présentes lors des manifestations prévues et de détecter les mouvements suspects à proximité des cibles vulnérables ou en lien avec celles-ci. Il est possible que, combinées aux autres renseignements connus, les images recueillies à l'aide des UAS permettent de confirmer qu'une attaque se prépare en vue de perturber un événement où une grande foule est attendue;
- Détecter les agents chimiques, biologiques, radiologiques ou nucléaires (CBRN) que des groupes terroristes pourraient tenter d'utiliser contre des cibles vulnérables. Diverses avancées technologiques ont permis d'équiper les UAS de capteurs qui peuvent être réglés de manière à détecter certains agents CBRN.

Cela dit, certaines restrictions importantes s'appliquent lors de la conception et de l'utilisation des UAS aux fins susmentionnées :

- Lorsque les UAS sont utilisés pour protéger des lieux vulnérables ou d'autres sites, notamment pour y assurer une surveillance, il est essentiel que cette utilisation soit légale, impérative et proportionnelle afin d'éviter de porter indûment atteinte aux droits humains fondamentaux, y compris au droit à la vie privée;
- Il convient de s'assurer que les opérations de surveillance par UAS ne sont pas influencées par des préjugés (sexistes, raciaux, religieux ou autres) pour éviter de victimiser ou stigmatiser davantage les communautés vulnérables;

- Il semble tout particulièrement impératif de faire preuve de retenue et de respecter toutes les garanties procédurales applicables, conformément aux normes et obligations internationales, dans la mesure où les UAS sont équipés de technologies de reconnaissance faciale[43].

Étude de cas 9.
Utilisation des systèmes de drone aérien pour prévenir les attaques terroristes – Costa Rica

Comme le Costa Rica accueille plusieurs événements internationaux qui attirent un grand nombre de visiteurs, ses cibles vulnérables peuvent être exposées à des menaces terroristes. Une partie des ses mesures préventives repose sur les technologies liées aux UAS :

- Les UAS sont utilisés pour assurer la protection des lieux, notamment pour repérer les vulnérabilités qui ne seraient pas visibles depuis le sol;
- Lors de grandes manifestations, les images captées par les UAS sont retransmises en direct au poste de commandement afin de donner une appréciation de la situation non seulement sur le site, mais aussi dans les zones environnantes;
- Les UAS sont également utilisés pour effectuer des patrouilles aux frontières et surveiller, entre autres, les points de passage illégaux avant la tenue de grandes manifestations;

43 Divers problèmes techniques nuisent encore à l'efficacité des systèmes de reconnaissance faciale installés sur les UAS, comme trouver le bon angle sous lequel capter un visage ou obtenir des images de bonne qualité quand le drone est dans les airs. Qu'il soit en mouvement ou en vol stationnaire, les images ainsi produites compliquent le travail d'établissement de correspondances. Toutefois, malgré ces difficultés, certaines entreprises technologiques spécialisées dans les services de surveillance ont mis au point des UAS dotés de systèmes de reconnaissance faciale avancés. Alors que des demandes de brevet sont déposées, les services de maintien de l'ordre de certains pays envisagent également d'équiper leurs drones aériens de tels systèmes.

- Les infrastructures critiques, telles que les pipelines, font aussi l'objet d'une surveillance à l'aide d'UAS;
- Il est aussi courant d'assurer la bonne communication entre les différents organismes, notamment avec la Direction générale de l'aviation civile, dans le but d'échanger des renseignements et de tenir chaque organisme informé.

Source : Intervention de M[me] Mercedes Quesada, Directrice des opérations liées aux UAS des services de renseignement du Costa Rica, à la réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

3.1.2 Forces de l'ordre

Les forces de l'ordre jouent plusieurs rôles importants pour ce qui est de prévenir les comportements terroristes liés aux UAS et d'enquêter sur ces derniers. Les forces de l'ordre, de par le soutien et les conseils qu'elles donnent aux exploitants de sites et de par leur autorisation à utiliser des technologies anti-UAS, sont des alliés indispensables pour assurer la protection des sites vulnérables.

Les sections qui suivent donnent un aperçu des aspects que les forces de l'ordre peuvent cibler dans leurs interventions pour atténuer les risques, contribuer à la réduction des dommages en cas d'incidents et poursuivre les auteurs présumés, notamment en cherchant à démanteler les réseaux criminels sous-jacents, tout au long du processus de planification de la sécurité.

Encadré 7.
Le respect des droits humains et des libertés fondamentales dans les opérations de maintien de l'ordre faisant appel aux systèmes de drone aérien

Les technologies liées aux UAS se répandent très rapidement, mais leur utilisation dans les opérations de maintien de l'ordre et de lutte contre le terrorisme soulève des préoccupations importantes du point de vue des droits humains[44]. Les États doivent donc analyser avec soin si le recours aux UAS est nécessaire et justifié, tant aux stades de la planification et de l'exécution qu'au stade de l'enquête subséquente. Parallèlement, même lorsque les autorités publiques collaborent avec d'autres États au maintien de l'ordre, elles doivent s'assurer que le transfert et la prolifération des technologies de drones ne se font pas au détriment des droits humains. En particulier :

1. L'utilisation des UAS au niveau national pour assurer le maintien de l'ordre, y compris la protection des cibles vulnérables, doit être pleinement conforme aux obligations qui incombent aux États en vertu du droit international des droits humains, notamment :

44 En 2020, la Rapporteuse spéciale sur les exécutions extrajudiciaires, sommaires ou arbitraires a rapporté qu'au moins 102 pays disposent d'un parc de drones actifs et qu'environ 40 pays possèdent ou sont en passe d'acquérir des drones armés.

(suite)

a) Le droit à la vie, lorsque les technologies de drones armés sont utilisées ou que les UAS servent à soutenir des stratégies policières de plus grande envergure qui prévoient le recours à la force[45];

b) Le droit à la vie privée, lorsque les technologies de drones sont utilisées aux fins de surveillance;

c) La liberté d'expression et la liberté d'association, qui sont indirectement touchées par la surveillance à distance généralisée que permettent les UAS.

2. Les obligations liées à la protection des droits humains ont des implications concrètes pour la planification d'opérations faisant appel aux UAS et des enquêtes concernant toute violation présumée :

a) Lors de la planification d'opérations faisant appel aux UAS : les États doivent s'assurer qu'une intervention est nécessaire et proportionnelle aux objectifs fixés. Une analyse rigoureuse doit être effectuée avant de décider d'utiliser des UAS qui peuvent offrir une capacité de ciblage. Il ne suffit pas d'avoir des plans et des ordres généraux qui exigent de cibler certains individus importants, il doit exister un lien direct entre les personnes ciblées et les menaces imminentes pour les autres;

b) Lors d'une enquête sur des violations présumées du droit à la vie : l'enquête doit être rapide, efficace et rigoureuse. Les personnes qui ont connaissance d'une violation potentielle du droit à la vie sont tenues de la signaler rapidement à leur hiérarchie. En outre, les enquêtes et les personnes qui les mènent doivent être indépendantes de toute influence indue et perçues comme telles.

3. Les États doivent être conscients des problèmes importants que pose le transfert des technologies de drones à des États qui ne respectent pas comme il se doit les droits humains. Conformément au droit international, les États doivent s'assurer qu'ils ne permettent pas à d'autres – intentionnellement ou par manque de

45 Le droit à la vie entre en ligne de compte aussi bien lorsque les UAS sont armés que lorsqu'ils ne le sont pas mais que les forces de l'ordre les utilisent pour soutenir des opérations au sol nécessitant le recours à la force. Les UAS de surveillance peuvent être armés facilement et à peu de frais. Les fabricants de drones vendent apparemment des modèles équipés de pistolets électriques ou de pulvérisateurs de gaz poivré et de gaz lacrymogènes aux services de police aux États-Unis, en Afrique du Sud, en France et en Inde.

diligence – d'utiliser illégalement des technologies de drones armés[46]. En outre, une fois que ces technologies commencent à se répandre largement dans le monde, il devient de plus en plus difficile d'en contrôler la propagation auprès d'acteurs non étatiques.

Source : Intervention de M^me^ Fionnuala Ní Aoláin, Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, à la réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

3.1.2.1 Soutenir les exploitants de cibles vulnérables

Comme la nature des menaces que posent les UAS est encore sous-estimée et relativement peu connue, les forces de l'ordre ont un rôle important à jouer auprès des exploitants de cibles vulnérables pour les aider à reconnaître et à comprendre les menaces particulières qui pèsent sur leurs locaux et leurs installations. Dans le cadre du cycle de gestion des risques, en particulier, ce soutien peut prendre les formes suivantes :

- Aide à l'élaboration d'un plan de sécurité, en commençant par le recensement des menaces et des vulnérabilités;
- Orientation et formation offertes au personnel du site sur l'exécution du plan;
- Conseils d'experts sur les mesures de gestion des risques possibles et les sources de financement disponibles pour aider à améliorer la sécurité.

En ce qui concerne la préparation aux crises, les services de police locaux doivent travailler en étroite collaboration avec les exploitants de sites à l'élaboration des plans d'urgence à appliquer dans le cas où des UAS armés parviennent à contourner les mesures de sécurité en place. Il faut avant tout veiller à évacuer aussi rapidement que possible le public et le personnel du site de la zone menacée. Il peut être bon d'encourager la tenue d'exercices d'évacuation réguliers, sous la supervision des policiers et du personnel du site chargé de la sécurité, simulant des scénarios de crise précis afin de faciliter l'évacuation en cas de crise réelle.

En outre, il est recommandé d'élaborer une matrice des risques à intégrer aux plans de sécurité afin de se préparer à intervenir en cas de crise liée à l'utilisation de drones. Les policiers, le personnel de sécurité et les autres intervenants auront une meilleure appréciation de la situation et pourront intervenir plus efficacement s'ils acquièrent les connaissances requises avant qu'une crise ne se produise.

46 Il s'agit là d'un problème particulièrement important, étant donné que les États allèguent régulièrement que les frappes de drones armés servent leurs objectifs antiterroristes, alors que, comme le souligne invariablement la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, ils invoquent souvent ce motif pour couvrir des activités illicites à l'appui de programmes nationaux partisans.

Encadré 8.
Intégration des informations recueillies à l'aide des systèmes de drone aérien dans le travail des centres de centralisation du renseignement

L'objectif ultime des centres de centralisation du renseignement est d'améliorer l'échange d'informations et la coopération interinstitutions en regroupant les informations provenant de multiples services de renseignement et services de police locaux, nationaux et même internationaux. Dans ce contexte, les UAS pourraient constituer une autre source d'informations utiles dans la lutte antiterroriste. Les capacités de renseignement, de surveillance et de reconnaissance des UAS pourraient être particulièrement utiles à ces centres lorsqu'ils recueillent des renseignements généraux et, plus spécifiquement, des informations relatives aux frontières ou des données essentielles à la protection des sites vulnérables et des infrastructures critiques.

Par exemple, l'une des principales responsabilités de l'Organe de coordination pour l'analyse de la menace (le centre de centralisation du renseignement de la Belgique) est de déterminer le niveau de menace national et de produire des analyses de menace coordonnées pour les infrastructures critiques du pays et celles de l'Union européenne. Les informations obtenues au moyen d'UAS peuvent contribuer à l'exécution de cette responsabilité.

Toutefois, le piratage d'UAS est un risque à ne pas écarter. En faisant partie du réseau de transmission de renseignements aux centres, les systèmes pourraient être utilisés par des pirates pour accéder aux informations stockées. Une analyse constante des failles de sécurité potentielles dans les logiciels utilisés et l'application des correctifs appropriés permettraient d'atténuer considérablement ce risque.

Source : « Commercial Unmanned Aircraft Systems in Counter-Terrorism Contexts » (les UAS commerciaux dans la lutte antiterroriste), manifestation parallèle organisée le 29 juin 2021 par le Bureau de lutte contre le terrorisme dans le cadre de la Semaine virtuelle de la lutte contre le terrorisme (télévision Web des Nations Unies, https://media.un.org/en/asset/k1g/k1gt7x766e).

3.1.2.2 Protection des cibles vulnérables à l'aide des technologies de lutte contre les systèmes de drone aérien

En pratique, les technologies anti-UAS peuvent être divisées en deux catégories selon leur objectif : les technologies de détection et les technologies de neutralisation/interception[47].

- *Technologies de détection des UAS :* contrairement aux observations à vue, ces technologies offrent un moyen nettement plus précis et fiable de repérer la présence d'un UAS menaçant dans un rayon donné en faisant appel, notamment, à des analyses par radiofréquence, à des capteurs acoustiques ou optiques, ou à des radars. Chacune de ces technologies présente des avantages et des inconvénients, et il appartient au personnel autorisé chargé du maintien de l'ordre et de la sécurité de les évaluer selon divers facteurs, comme le coût, la facilité de déploiement et le contexte dans lequel elles sont censées être utilisées (par exemple, les niveaux de bruit et d'encombrement des fréquences radio, l'éclairage et les conditions atmosphériques)[48]. Ces technologies de détection peuvent, par exemple, être contrées en couvrant l'émetteur GPS du drone avec un matériau comme de l'aluminium. Les exploitants de cibles vulnérables doivent donc continuer à mettre en place des niveaux de sécurité multiples (incluant l'observation humaine/visuelle), même lorsqu'ils utilisent des technologies anti-UAS très efficaces.
- *Technologies de neutralisation/interception des UAS :* une fois que la présence d'un UAS menaçant a été détectée, le personnel autorisé chargé du maintien de l'ordre et de la sécurité doit rapidement déterminer les mesures les plus appropriées à prendre pour empêcher l'appareil de causer des blessures ou des dommages. Les technologies de neutralisation/interception des UAS se divisent en deux grandes catégories : cinétiques et non cinétiques. Celles de la première catégorie, qui visent à éliminer ou à réduire la menace que pose l'objet

47 Les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité fournissent également un aperçu des différentes technologies de détection et de neutralisation/interception et fait état, notamment, des facteurs que les forces de l'ordre doivent considérer lorsqu'elles utilisent les technologies à leur disposition. Voir sous-module II, section 3.1 sur les systèmes et les techniques de lutte contre les UAS.

48 L'efficacité des dispositifs radiofréquences pour détecter les signaux servant à contrôler les UAS, par exemple, diminue considérablement dans les zones densément peuplées, où le bruit et l'encombrement des fréquences sont plus importants. Le microphone des capteurs acoustiques offre des capacités de détection limitées dans les milieux bruyants, alors que l'efficacité des technologies de reconnaissance optique peut être compromise lorsque l'éclairage est faible. Les systèmes radars, qui sont le principal moyen de détection à longue portée, sont également capables de repérer les UAS de petite taille ou volant à basse altitude, mais ils ont souvent du mal à faire la distinction entre un oiseau et un petit drone [Association of the United States Army (2021)].

volant, font généralement appel à des fusils à filet, à des dispositifs de lancement de projectiles ou à des armes laser. En revanche, celles de la deuxième catégorie ont pour but de brouiller les signaux des UAS (en utilisant, par exemple, des micro-ondes de forte puissance). Les mesures non cinétiques, qui visent à compromettre la manœuvre des UAS, reposent souvent sur l'émission de signaux de radiofréquence.

De nombreuses technologies anti-UAS, notamment celles destinées à compromettre les opérations des UAS, ne sont généralement pas accessibles aux exploitants de sites vulnérables. L'utilisation de technologies de neutralisation/interception constitue donc, dans bien des cas, une prérogative pour les forces de l'ordre et les autres membres du personnel de sécurité ou des services publics autorisés, qui doivent connaître les avantages et les inconvénients des solutions offertes et s'assurer qu'elles sont déployées conformément aux cadres juridiques applicables ainsi qu'aux contextes particuliers dans lesquels elles seront utilisées. Une étroite collaboration avec les exploitants de cibles vulnérables s'impose afin de comprendre les caractéristiques physiques et techniques des sites et des zones environnantes[49]. En outre, il est recommandé d'évaluer régulièrement les technologies anti-UAS afin de déterminer si leur inclusion dans les protocoles de sécurité contribue à sécuriser les sites ou s'il ne fait que créer un besoin auquel on ne peut pas répondre indéfiniment. Le déploiement de technologies anti-UAS lors d'une grande manifestation exige également une bonne compréhension de la dynamique de l'événement en question (étapes, déplacements attendus des participants, arrivée et départ des dignitaires, etc.).

49 Par exemple, il peut être plus approprié d'utiliser certaines technologies en milieu rural et d'autres en milieu urbain.

Encadré 9.
Systèmes de drone aérien et raids jusqu'au point d'origine

Une fois qu'un système de drone aérien a été détecté et neutralisé, diverses technologies peuvent être utilisées pour retracer ses signaux jusqu'à leur point d'origine et remonter jusqu'à l'emplacement d'où il était piloté. Cette mesure peut permettre aux forces de l'ordre de non seulement neutraliser un appareil hostile, mais aussi d'appréhender les utilisateurs tout en obtenant des renseignements essentiels sur les terroristes et les bases de commandement et de contrôle.

Les systèmes de drone aérien peuvent également être coordonnés avec les centres de centralisation du renseignement pour optimiser les raids jusqu'au point d'origine. Les informations que les États Membres obtiennent sur les terroristes lors de tels raids pourraient ensuite être analysées et traitées dans un centre national de centralisation du renseignement (voir encadré 8) en vue d'une diffusion rapide et précise aux services de police ou de renseignement concernés.

Source : « Commercial Unmanned Aircraft Systems in Counter-Terrorism Contexts » (les UAS commerciaux dans la lutte antiterroriste), manifestation parallèle organisée le 29 juin 2021 par le Bureau de lutte contre le terrorisme dans le cadre de la Semaine virtuelle de la lutte contre le terrorisme (télévision Web des Nations Unies, https://media.un.org/en/asset/k1g/k1gt7x766e).

Étude de cas 10.
Mise à l'essai et évaluation des contre-mesures visant les drones – INTERPOL et police norvégienne

Du 28 au 30 septembre 2021, INTERPOL et la police norvégienne ont organisé un exercice de trois jours réunissant des experts des services chargés de l'application de la loi, du monde universitaire et du secteur industriel venus d'Europe, d'Israël et des États-Unis pour évaluer et tester 17 contre-mesures visant les drones afin d'assurer la sécurité d'un environnement aéroportuaire par la détection, le suivi et la reconnaissance des drones, ainsi que l'identification de leurs pilotes[50].

Chaque contre-mesure a été évaluée et notée en fonction de critères précis. Les conclusions pourront ainsi être rassemblées afin de créer un cadre INTERPOL de lutte contre les drones, qui établira un point de convergence mondial pour la collaboration et le partage des connaissances entre les services chargés de l'application de la loi des 194 pays membres d'INTERPOL.

L'exercice s'est déroulé à l'aéroport d'Oslo Gardermoen en pleine activité. Pour être exploité dans l'aéroport, chaque système devait être autorisé et approuvé par l'organisme de réglementation, et l'autorisation de l'exploitant de l'aéroport devait être obtenue. En raison de sa complexité, l'exercice a nécessité une étroite collaboration avec le propriétaire de l'aéroport, l'Autorité norvégienne des communications, l'Autorité de l'aviation civile et UAS Norway, qui a permis de s'assurer d'une part que tous les systèmes et tous les tests étaient conformes aux normes requises et d'autre part qu'ils ne perturberaient pas les activités de l'aéroport.

Outre les exercices, des ateliers et des exposés sur les incursions de drones axés sur la conservation des éléments de preuve ont également été organisés. Au cours de ces séances, les participants ont échangé des bonnes pratiques et réfléchi aux solutions futures potentielles contre les incursions de drones.

Sources : www.interpol.int/fr/Actualites-et-evenements/Actualites/2021/INTERPOL-procede-a-un-exercice-grandeur-nature-pour-tester-les-contre-mesures-visant-les-drones; intervention de M. Christopher Church, Spécialiste de haut niveau en criminalistique mobile chez INTERPOL, à la réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

50 Les contre-mesures testées, qui étaient réparties en quatre groupes (mesures passives, actives, multisystèmes et d'exécution), ont été évaluées en fonction de leur capacité à détecter, à suivre et à localiser les drones entrant dans l'espace aérien réglementé. Au cours de cette période, plus de 2 000 mouvements d'aéronefs actifs ont été effectués.

Étude de cas 11.
Utilisation des systèmes de drone aérien par la police de la Catalogne (Espagne)

Lors du congrès mondial de la téléphonie mobile tenu à Barcelone en 2018, le service de police autonome (« Mossos d'Esquadra ») de la Catalogne (Espagne) a déployé pour la première fois un UAS de surveillance afin d'assurer la sécurité de l'événement. Le déploiement était régi par la nouvelle loi espagnole sur les drones (décret royal 1036/2017), qui autorise les forces de sécurité à utiliser des appareils sans pilote dans diverses opérations, en particulier dans l'espace aérien contrôlé, au-dessus des personnes et des bâtiments, et la nuit. Les drones déployés par la police régionale prennent des photos et enregistrent des vidéos en direct dans les zones surveillées.

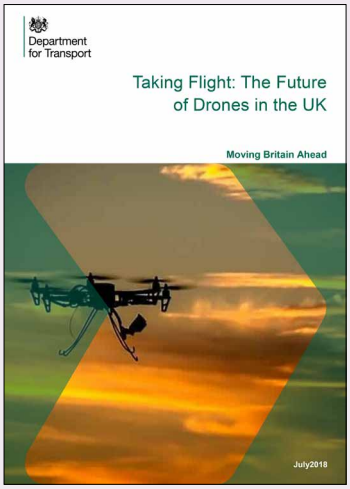
Les agents de la police régionale de Barcelone ont également mené des opérations à proximité de l'aéroport de la ville (El Prat), en collaboration avec la société des aéroports espagnols (AENA – Aeropuertos Españoles y Aeronavegación Aérea) et ENAIRE (le fournisseur de services de circulation aérienne de l'Espagne). Ces opérations ont été réalisées dans une zone d'une hauteur définie de 50 mètres, en étroite coordination avec les services d'hélicoptères, et un contact permanent a été maintenu avec la tour de contrôle de l'aéroport.

Source : www.unmannedairspace.info/uncategorized/barcelona-security-forces-pioneer-urban-drone-services-spain/.

Outil 7.

Bonnes pratiques et mesures de sécurité lors du déploiement de technologies de lutte contre les systèmes de drone aérien – Ministère des transports du Royaume-Uni (2018)

(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729458/taking-flight-the-future-of-drones-in-the-uk.pdf)

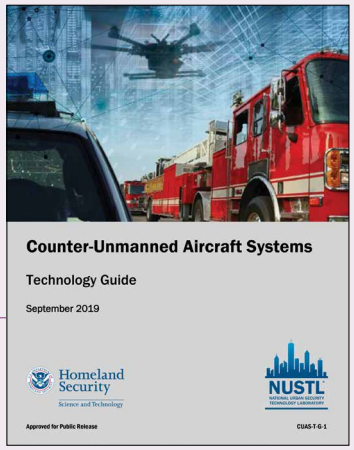


Dans un document de consultation élaboré en 2018, le Ministère des transports du Royaume-Uni reconnaît la nécessité de mettre en place diverses mesures permettant d'assurer l'utilisation appropriée des UAS, tant à des fins de détection que de neutralisation/interception[51] :

- Seuls les exploitants dûment formés/autorisés peuvent utiliser la technologie des drones;
- L'utilisation de la technologie doit avoir une portée et un but précis, et il doit y avoir une politique opérationnelle propre à chaque site conforme à la législation applicable (par exemple, un code de pratique défini);
- S'il y a lieu, une évaluation complète des risques est réalisée conformément à la législation sur la santé et la sécurité;
- Le cas échéant, un protocole d'accord peut être établi avec les organismes de réglementation compétents au sujet des mécanismes de règlement des différends et de la résolution des difficultés résultant d'un dysfonctionnement ou d'une mauvaise utilisation de la technologie;
- Toutes les données saisies à l'aide de la technologie de détection des drones sont gérées conformément à la législation applicable, telle que les règlements sur la protection des données;
- La technologie n'est déployée que si un besoin opérationnel en justifie une utilisation proportionnelle, conformément à la législation applicable, y compris celle relative aux droits humains (par exemple, l'article 8 de la Convention européenne des droits de l'homme);
- Des tests ont été réalisés pour vérifier l'adaptation à la finalité de la technologie, le but étant de réduire au minimum les interférences accidentelles;
- Les organismes de réglementation chargés de surveiller la technologie déployée sont informés de son installation avant les faits, dans la mesure du possible;
- Selon le type de site ou d'événement, les organisations ont recours à des communications publiques, à la mobilisation communautaire et à la signalisation pour prévenir le public que l'utilisation non autorisée de drones sera surveillée et pourrait faire l'objet de mesures coercitives;
- Une assurance appropriée est contractée.

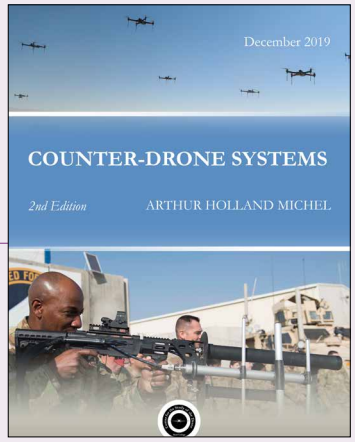
51 Voir *Taking Flight: The Future of Drones in the UK* (Prendre son envol : l'avenir des drones au Royaume-Uni), par. 7.21 et 7.38.

Outil 8.
Counter-Unmanned Aircraft Systems: Technology Guide (Guide sur les technologies de lutte contre les systèmes de drone aérien) – Département de la sécurité intérieure des États-Unis (2019)
(www.dhs.gov/publication/st-c-uas-technology-guide)



Ce guide technique vise à renseigner les premiers secours sur les technologies anti-UAS. Il fournit un aperçu des technologies de petits systèmes de drone aérien et de leurs principaux composants. On y retrouve, notamment, une expertise technique, scientifique et d'ingénierie offerte par le National Urban Security Technology Laboratory, ainsi que des informations tirées de recherches sur Internet, de publications spécialisées et de données des fabricants.

Outil 9.
Counter-Drone Systems (Systèmes anti-drones) – Center for the Study of the Drone du Bard College (2019)
(https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf)



Ce rapport fournit des renseignements généraux sur le fonctionnement et la demande croissante de technologies anti-UAS, présente une base de données des produits anti-UAS connus dans le monde et explique certains des problèmes posés par ces technologies. L'analyse réalisée s'appuie sur divers éléments : recherches en libre accès dans des rapports techniques et politiques, des témoignages écrits, des articles d'actualité, des projets d'analyse et des données des fabricants; entrevues de fond avec des représentants du gouvernement, des forces de l'ordre et du secteur et des experts en la matière; participation à des conférences et à des ateliers publics et fermés.

3.1.2.3 Enquêtes sur les incidents impliquant des UAS

Les personnes qui enquêtent sur les attaques impliquant des UAS doivent respecter les procédures générales prévues dans la législation pénale nationale (en ce qui concerne notamment les techniques d'enquête, les arrestations et les mandats d'arrêt, et le niveau de preuve) mais font souvent face à des situations ou à des difficultés qu'elles ne rencontrent pas nécessairement dans les enquêtes pénales ou antiterroristes courantes. Il est important que les forces de l'ordre comprennent les particularités des

attaques impliquant des drones et mobilisent un ensemble approprié de compétences en matière d'investigation qui faciliteront, notamment, la gestion de la scène de crime et l'enquête sur les réseaux criminels/terroristes sous-jacents.

- *Gestion de la scène de crime :* les enquêtes sur les incidents impliquant des drones doivent être menées le plus tôt possible afin de diminuer les risques de contamination de la scène de crime. Les appareils récupérés au sol, une fois rendus inoffensifs, peuvent fournir des éléments de preuve utiles à l'appui des procédures pénales. Alors que les experts en criminalistique numérique ont un rôle essentiel à jouer dans l'extraction des données des systèmes de drone aérien (vitesse, altitude, coordonnées GPS, enregistrements de vol, etc.), d'autres peuvent rechercher des preuves matérielles traditionnelles, comme des empreintes digitales et des échantillons de matières biologiques, laissées sur des composants, notamment sur les dispositifs de commande abandonnés. De même, les auteurs des faits peuvent avoir laissé des éléments de preuve utiles à l'endroit d'où ils ont mené l'attaque, en particulier s'ils ont dû quitter leur poste à la hâte[52].

Encadré 10.
Le danger potentiel des systèmes de drone aérien retrouvés au sol – nord de l'Iraq

Les forces de l'ordre et autres agents autorisés doivent faire preuve d'une grande prudence lorsqu'ils manipulent des UAS retrouvés au sol, car ceux-ci peuvent avoir des visées offensives même s'ils semblent, en apparence, sans danger. Une situation du genre s'est produite dans le nord de l'Iraq, où des membres de milices kurdes ont abattu un drone de la taille d'un modèle réduit d'avion en pensant qu'il s'agissait d'un des nombreux drones de reconnaissance de Daech. Ils ont décidé d'examiner l'appareil de plus près pour tenter d'obtenir des informations sur les activités terroristes perpétrées à l'aide de drones. Toutefois, ils auraient dû être plus prudents : au moment de désassembler l'appareil, une détonation a été provoquée par un petit engin explosif improvisé dissimulé.

Source : Staniforth (2017).

- *Enquête sur les réseaux sous-jacents :* dans la plupart des incidents impliquant des UAS, « un attaquant aura bénéficié de l'aide d'autres personnes, par le biais d'un réseau ou d'un groupe terroriste plus large qui l'aura aidé à se procurer la technologie nécessaire pour exploiter des systèmes d'aéronefs non habités, à choisir ses cibles et à perpétrer l'attentat, ou qui lui aura prêté assistance après l'attentat. L'identification de ces réseaux est essentielle pour empêcher que le même groupe, ou des groupes affiliés, commettent de nouveaux attentats au moyen de systèmes d'aéronefs non habités ou d'autres armes. » [Bonne pratique n° 20, Forum mondial de lutte contre le terrorisme (2019)]. Au moment de déterminer l'ampleur et les ramifications de l'opération

52 Voir les directives techniques pour l'application de la résolution 2370, sous-module II, en particulier les sections 3.2 (sécurité sur la scène d'incidents impliquant des UAS), 3.3 (rassemblement et conservation des éléments de preuve), 3.4 (exploitation technique des UAS et des composants récupérés) et 3.5 (gestion des informations).

criminelle ayant conduit à une attaque par UAS, la licence des exploitants, l'enregistrement des UAS et les documents de contrôle des exportations peuvent fournir des pistes d'enquête importantes, à moins que les auteurs n'aient utilisé des UAS sur mesure[53].

Dans la mesure où les ressources le permettent, les enquêtes doivent également porter sur le réseau sous-jacent de complices et sur les personnes impliquées dans la préparation de l'attentat. Une enquête approfondie peut mettre au jour la présence d'éléments et de liens transnationaux, à condition que les enquêteurs veuillent et puissent obtenir des renseignements et des éléments de preuve auprès de leurs homologues étrangers, notamment par l'intermédiaire des mécanismes d'entraide judiciaire.

Encadré 11.
La conspiration des entreprises IBACS – plusieurs pays

Dans au moins quatre pays (Bangladesh, Danemark, Espagne et Royaume-Uni), des enquêtes ont mis en lumière la vaste portée transnationale et les rouages complexes du programme d'UAS de Daech. Dans le cadre de ce programme, plusieurs sociétés écrans spécialisées en informatique, en électronique et en services Web ont été créées en 2015 au Royaume-Uni, au Bangladesh et en Espagne pour acheter des équipements d'UAS et les transférer à Daech. Les achats ont été effectués aux États-Unis et au Canada auprès d'au moins neuf entreprises différentes. Pour que leurs activités semblent légitimes, les conspirateurs ont utilisé des noms d'emprunt et des applications de messagerie cryptée afin de ne pas être repérés par les services de police.

Source : Rassler (2018).

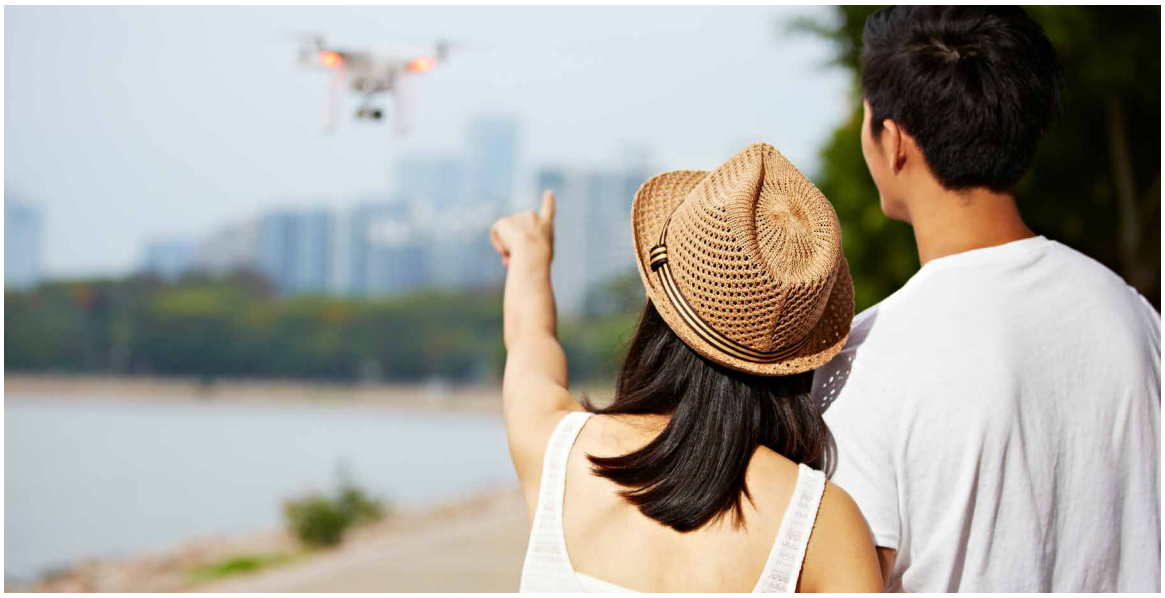
53 Voir les directives techniques pour l'application de la résolution 2370, sous-module II, en particulier la section 3.6 sur l'identification des auteurs.

Étude de cas 12.
Pouvoir d'interpellation et de fouille à l'égard des systèmes de drone aérien

En 2018, le Ministère de l'intérieur du Royaume-Uni a publié un document de consultation publique intitulé « Stop and Search: Extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers and corrosive substances » (Interpellation et fouille : extension des pouvoirs des policiers aux infractions impliquant des drones, des pointeurs laser et des substances corrosives). On y retrouve le scénario hypothétique suivant qui illustre un cas typique où les sites peuvent se retrouver d'autant plus vulnérables aux attaques impliquant des UAS si les policiers ne sont pas investis de pouvoirs d'interpellation et de fouille liés aux drones :

« La police a reçu de multiples signalements du public l'informant qu'un individu utilise un drone dans un secteur habité, ce qui constitue une infraction au décret sur la navigation aérienne 2016 (Air Navigation Order 2016). Elle a en main une description de l'individu et de l'endroit. Les agents patrouillent dans le secteur à l'heure où la plupart des appels concernant l'incident ont été reçus et identifient l'individu correspondant à la description. Bien qu'il ne pilote pas de drone, les agents, constatant qu'il transporte un grand sac, décident de s'approcher et de lui demander ce qu'il fait là. Pendant l'échange, l'individu se montre évasif et semble tenir nerveusement le sac fermé. Compte tenu de l'endroit, de l'heure et de la description et du comportement de l'individu, les agents estiment avoir des motifs raisonnables de soupçonner que ce dernier est en possession d'un drone qu'il a utilisé dans un secteur habité, contrevenant ainsi au décret sur la navigation aérienne 2016. Les agents expliquent pleinement et clairement à l'individu les motifs et l'objet de la fouille avant de procéder et saisissent finalement le drone et les articles connexes. »

Source : Ministère de l'intérieur du Royaume-Uni (2018).



Outil 10.
Cadre d'intervention en cas d'incident lié à un drone : À l'intention des premiers intervenants et des professionnels de la criminalistique numérique – INTERPOL (2020)
(www.interpol.int/fr/content/download/15298/file/DFL_DroneIncident_Final_FR.pdf)

Ce guide, qui fournit des conseils techniques pour gérer et traiter un incident lié à un drone, a été conçu pour deux types de publics : d'une part, les premiers intervenants et les policiers qui assistent aux incidents; d'autre part, les professionnels de la criminalistique numérique qui traitent les éléments de preuve électroniques après l'incident. Les procureurs, les juges et les avocats peuvent aussi en tirer parti.

Les conseils fournis doivent être utilisés comme références aux niveaux stratégique et tactique et s'accompagnent d'extraits du *Crime Scene Investigation Guide* (Guide d'enquête sur les scènes de crime), publié par le National Forensic Science Technology Center des États-Unis[54]. Les différentes sections du guide portent, notamment, sur les composants et les charges utiles des drones, les données fournies, les sources d'éléments de preuve (téléphone, télécommande, carte mémoire, stockage interne), les procédures de sécurité, les précautions à prendre avant de s'approcher d'un drone ou de manipuler un appareil, les premiers secours et les procédures d'urgence, le processus de saisie d'un drone, les enquêtes en criminalistique numérique, la préservation des empreintes digitales, et la collecte et la conservation des éléments de preuve numériques.

3.1.2.4 Douanes et maintien de l'ordre aux frontières

Les UAS présentent un intérêt du point de vue des douanes et du maintien de l'ordre aux frontières dans au moins trois domaines liés à la prévention du terrorisme[55] :

- La détection et la saisie des UAS et de leurs composants passés en contrebande en vue de servir des visées terroristes;
- La détection et la saisie des UAS devant servir à transporter les armes, les marchandises, l'équipement, l'argent, etc. qui seront utilisés pour planifier des actes terroristes;
- L'utilisation d'UAS par les services frontaliers en tant qu'outils de répression pour surveiller les activités transfrontalières et repérer, notamment, les personnes qui traversent illégalement les frontières dans des zones reculées et poreuses entre les points d'entrée établis[56].

54 Voir https://nij.ojp.gov/topics/articles/crime-scene-investigation-guides-law-enforcement.

55 Voir les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité, sous-module II, section 2.3.1 sur les douanes et les contrôles frontaliers.

56 Les UAS peuvent être utilisés pour obtenir d'importantes informations visuelles et faciliter la surveillance des frontières poreuses grâce à leur capacité à détecter sur de grandes distances tout élément suspect pouvant représenter une menace terroriste. En outre, les systèmes équipés de capteurs infrarouges ou thermiques peuvent aider les équipes de patrouille à sécuriser les zones frontalières la nuit.

Les articles à double usage (comme les composants matériels et les logiciels)[57] présentent, pour les autorités douanières, un défi sensiblement pareil à celui du commerce de substances pouvant également servir à la fabrication d'engins explosifs improvisés, comme le nitrate d'ammonium. Là encore, le succès dépend de la capacité à échanger et à traiter des informations préalables précises concernant les articles entrants et à mettre en place des mécanismes d'alerte[58].

3.1.3 Services de renseignement

L'effort global d'atténuation des risques repose fondamentalement sur la capacité des pays à comprendre la dynamique et le fonctionnement des réseaux illégaux d'approvisionnement en UAS, à en identifier les acteurs et à déterminer le parcours emprunté (en ligne et hors ligne) par les personnes et les marchandises visées. Parallèlement, pour mobiliser les ressources nécessaires au démantèlement des chaînes d'approvisionnement servant à alimenter les activités terroristes liées aux UAS, les pays doivent être en mesure de recueillir et de traiter des volumes importants de renseignements de grande qualité. Les renseignements obtenus auprès de diverses sources doivent être traités en comparant toutes les données disponibles.

Par exemple, des cadres réglementaires appropriés peuvent être mis en place pour obliger les vendeurs d'UAS à exercer une diligence raisonnable à l'égard des clients potentiels et à signaler les transactions suspectes aux autorités compétentes (voir section 3.2.3). Cela permettrait d'obtenir des informations utiles qui pourraient ouvrir de nouvelles pistes d'enquête ou confirmer la validité de celles explorées, ou encore fournir un nouvel éclairage sur les opérations en cours et les suspects.

Des informations cruciales peuvent également être obtenues sur le terrain, notamment dans les zones de conflit, en recueillant et en analysant des preuves photographiques et

57 Le Régime de contrôle de la technologie des missiles (RCTM) et l'Arrangement de Wassenaar sont les deux instruments multilatéraux qui définissent le cadre normatif régissant le contrôle des exportations d'UAS. Le RCTM, qui compte 35 membres, est une initiative pour l'octroi de permis d'exportation afin de prévenir la prolifération d'UAS capables de transporter des armes de destruction massive. Les 42 pays ayant adhéré à l'Arrangement de Wassenaar contribuent notamment aux efforts visant à prévenir l'achat de biens à double usage par des terroristes, en contrôlant l'exportation de tous les articles figurant sur la Liste des biens et des technologies à double usage et la Liste des munitions pour empêcher qu'ils ne soient transférés ou retransférés illégalement.

58 Les directives techniques pour l'application de la résolution 2370 du Conseil de sécurité décrivent les types de sous-systèmes d'UAS que les États peuvent envisager de réglementer. Voir sous-module II, section 2.3.2 sur le contrôle des UAS et des principaux sous-systèmes.

documentaires. Dans certains cas, les gouvernements ont fait appel à des organisations privées qui, par l'entremise de leurs équipes d'enquête sur le terrain, ont documenté la présence d'armes, de munitions et autres matériels connexes illicites dans les zones de conflit et ont retrouvé les fournisseurs. Par exemple, des recherches récentes sur l'acquisition, la conception et l'utilisation d'UAS armés par Daech, en Iraq et en République arabe syrienne, ont mis en lumière son vaste réseau de fournisseurs de logiciels et de composants matériels utilisés dans l'assemblage d'UAS. Ces recherches ont également montré comment les groupes terroristes utilisent les marchés internationaux (notamment, ceux en ligne) pour se procurer des UAS et des composants connexes, ce qui explique l'attention croissante que les services de renseignement accordent à la surveillance des transactions sur Internet (voir encadré 12).

Encadré 12.
Réseau de fournisseurs de systèmes de drone aérien de Daech

L'enquête menée par Conflict Armament Research (CAR)[59] sur les UAS commerciaux récupérés en Iraq a permis de déterminer comment Daech a réussi à se procurer neuf d'entre eux. Un lien a d'abord été établi entre le numéro de série des appareils et certains des fournisseurs qui les avaient vendus.

Selon l'analyse approfondie du programme d'UAS de Daech réalisée par le Combating Terrorism Centre at West Point, « l'un des principaux points qui ressort de [l'enquête de CAR] est la complexité de l'approvisionnement en drones de Daech. En effet, sept des neuf drones commerciaux ont été achetés dans [cinq pays différents], qu'ils aient été achetés directement du fournisseur ou sur le Web [...]. Autre point intéressant : les différentes étapes qui marquent l'achat des neuf drones de l'État islamique. Dans plusieurs cas, le drone commercial a été acheté dans un pays, activé dans un autre, pour finalement être utilisé ailleurs (en Iraq ou en Syrie). »

Source : Rassler (2018).

59 CAR est un organisme d'enquête britannique qui surveille l'approvisionnement en armes classiques, en munitions et en matériel militaire connexe dans les zones touchées par des conflits.

3.2 Acteurs non étatiques

En travaillant de concert avec les acteurs institutionnels, les concepteurs de logiciels liés aux UAS et les fabricants de pièces détachées et de technologies anti-UAS peuvent tous contribuer à une collaboration multisectorielle visant à entraver l'achat et l'utilisation d'UAS à des fins terroristes. Par ailleurs, il est possible d'inciter les utilisateurs d'UAS, les exploitants de sites vulnérables, le public et les organisations de la société civile à prendre d'importantes mesures d'atténuation; pour ce faire, il faut mener des campagnes de sensibilisation ciblées, offrir une combinaison appropriée de mesures incitatives et établir des canaux de communication adéquats avec les forces de l'ordre et les autres autorités gouvernementales.

3.2.1 Exploitants de cibles vulnérables

Les propriétaires et les gestionnaires de sites vulnérables qui souhaitent protéger leur site contre le risque d'activités terroristes impliquant des UAS peuvent prendre diverses mesures importantes :

- *Inclure une évaluation des menaces et des vulnérabilités liées aux UAS dans le plan de sécurité du site :* il est primordial que les exploitants de cibles vulnérables s'assurent que leur plan de gestion du risque de terrorisme comprenne une évaluation des menaces et des vulnérabilités particulières liées aux UAS. On peut obtenir des informations utiles à l'élaboration du plan de sécurité en examinant les répercussions que les UAS ont eues sur des sites semblables par le passé, dans le pays ou ailleurs. Ces incidents peuvent fournir des informations clés sur les menaces et les vulnérabilités, qui permettront aux exploitants de choisir les mesures d'atténuation les plus appropriées[60].
- *Déterminer la nature et l'ampleur de la menace qui pèse sur le site :* tous les sites extérieurs devraient mettre en place de solides mesures pour lutter contre les drones; ceux qui n'ont que quelques points d'accès ouvert (les fenêtres d'un musée, par exemple) peuvent n'avoir qu'à considérer si des UAS pilotés à distance peuvent s'introduire dans ces espaces étroits.
- *Suivre l'évolution du marché des drones :* les connaissances que les exploitants de sites peuvent acquérir sur l'évolution technologique des UAS les aideront à mieux évaluer la nature et l'ampleur du risque. En se tenant au courant des nouvelles caractéristiques et capacités des UAS commerciaux ou de loisir qui font leur apparition sur le marché, ils seront aiguillés dans leurs considérations.
- *Choisir les solutions de détection et d'atténuation les plus appropriées :* il n'existe pas de procédé universel pour déterminer les mesures d'atténuation des risques les plus appropriées. Comme il y a des centaines de solutions sur le marché, il est souvent difficile pour les utilisateurs finaux de trouver celles qu'il leur convient le mieux. Le choix dépend des risques particuliers cernés dans un cadre d'exploitation donné, du budget, et même des sites de lancement potentiels dans les environs. Il faut repérer les endroits d'où un drone pourrait être piloté[61], les surveiller et les prendre en compte dans le plan de sécurité.

60 Les menaces liées aux UAS ne sont pas forcément statiques; elles sont potentiellement dynamiques, et les plans de gestion des crises doivent en tenir compte. Par exemple, un drone peut se poser à un endroit vulnérable du site pour se diriger l'instant d'après vers un autre point de vulnérabilité. Il peut même être utilisé pour pourchasser le public durant l'évacuation. En outre, l'évaluation des menaces ne doit pas exclure la possibilité que de petits UAS soient introduits clandestinement sur le site, puis activés de l'intérieur.

61 Parcs de stationnement, routes permettant de prendre facilement la fuite, emplacements surélevés offrant une bonne visibilité sur le site à protéger, etc.

- *Mettre en œuvre des solutions anti-UAS qui ne dépendent pas de la technologie :* la plupart des cadres réglementaires interdisent aux exploitants de sites de neutraliser un UAS, d'en prendre le contrôle ou d'en perturber le fonctionnement[62]. Il est donc essentiel pour les exploitants de bien comprendre comment l'utilisation des technologies anti-UAS est balisée[63]. Cependant, selon le cadre juridique applicable, ils peuvent mettre en place de manière autonome une série de mesures d'atténuation qui ne dépendent pas de ces technologies, comme les mesures suivantes :
  - *Dissimulation des biens vulnérables :* on peut utiliser des écrans non transparents, du feuillage, etc. pour rendre les biens vulnérables partiellement ou totalement invisibles depuis les airs. De même, il est possible de rendre moins attrayants les sites de lancement potentiels d'UAS dans les zones environnantes, en les dissimulant à la vue ou en les éclairant et en contrôlant l'accès. Ces mesures peuvent nécessiter une coordination avec les propriétaires et les gestionnaires des lieux, comme les municipalités, ainsi que leur autorisation et leur intervention.
  - *Surveillance du site :* les zones extérieures, comme les cours et les toits, peuvent faire l'objet d'un contrôle régulière afin d'y déceler la présence d'UAS ou d'objets largués depuis les airs. Il est essentiel de mettre en place des mesures d'atténuation contre l'interférence de drones qui soient efficaces en tout temps, et non uniquement lors de rassemblements ou de manifestations, dans la mesure où des UAS peuvent être utilisés pour larguer des dispositifs dangereux ou surveiller l'installation ciblée lorsque celle-ci est inoccupée ou fermée au public.
  - *Surveillance à vue/détection visuelle :* cette méthode de détection repose sur l'observation humaine de l'horizon pour y détecter la présence de tout UAS potentiellement menaçant. Lorsqu'un appareil est repéré à l'intérieur ou à proximité d'un endroit vulnérable, les exploitants du site se doivent d'alerter rapidement la police et le personnel de sécurité. Dans la mesure où les outils technologiques de détection ne sont pas infaillibles, la surveillance à vue devrait toujours être utilisée en combinaison avec ceux-ci, et non dans les seuls cas où ils ne sont pas accessibles.
  - *Outils de communication/mise en garde :* des panneaux et des avis de mise en garde devraient être affichés dans le voisinage et dans les pôles de transport pour signaler qu'il est interdit d'utiliser des UAS au-dessus de certaines cibles vulnérables. De telles mesures ne dissuaderont probablement pas les acteurs malveillants, mais elles pourraient aider à réduire les incidents de négligence. Les services de police et le personnel de sécurité pourraient ainsi consacrer plus efficacement leurs ressources et leur attention aux incidents problématiques, qui sont moins nombreux. En outre, on peut informer le public des numéros de téléphone à composer pour signaler toute activité suspecte; le site Web de l'exploitant du site et ses comptes de

62 Si l'utilisation de technologies de neutralisation/interception des UAS peut soulever des problèmes techniques et juridiques complexes, il existe de nombreux outils de détection (utilisant notamment la technologie radar) qui sont, juridiquement, à la portée des exploitants de sites, même si ces derniers doivent souvent en assumer les coûts. Grâce aux solutions de détection des UAS, les exploitants de sites pourront obtenir des informations essentielles, comme la vitesse, la taille, la capacité utile et le mode de navigation d'un objet menaçant, puis utiliser ces informations pour évaluer, entre autres, le risque de dommages collatéraux, ce qui influencera leur décision quant aux mesures d'atténuation appropriées.

63 Aux États-Unis, par exemple, les UAS font l'objet de mesures de protection semblables à celles prévues pour les appareils commerciaux ou de passagers puisqu'ils sont considérés comme des aéronefs. Ainsi, la loi fédérale américaine interdit de façon générale aux organisations privées et aux particuliers d'interférer avec des UAS en vol, notamment en brouillant leurs signaux.

médias sociaux peuvent également être mis à profit à cette fin[64].

  - *Renforcement des capacités liées à la détection et à la manipulation des UAS :* le personnel du site peut être sensibilisé aux risques que l'utilisation illégale d'UAS présente en fonction des activités du site. Une formation devrait également lui être dispensée sur la façon de détecter visuellement les incidents, de les signaler et de traiter les UAS suspects, aussi bien en vol qu'au sol. Selon la manière dont les employés traitent un UAS qui s'est écrasé au sol, ils risquent, notamment, de compromettre l'enquête qui s'ensuit, de briser la chaîne de possession des éléments de preuve, etc. (voir section 3.1.2.3). En attendant l'intervention des policiers, le personnel du site peut simplement prendre des photographies de l'incident ou l'enregistrer sur vidéo.

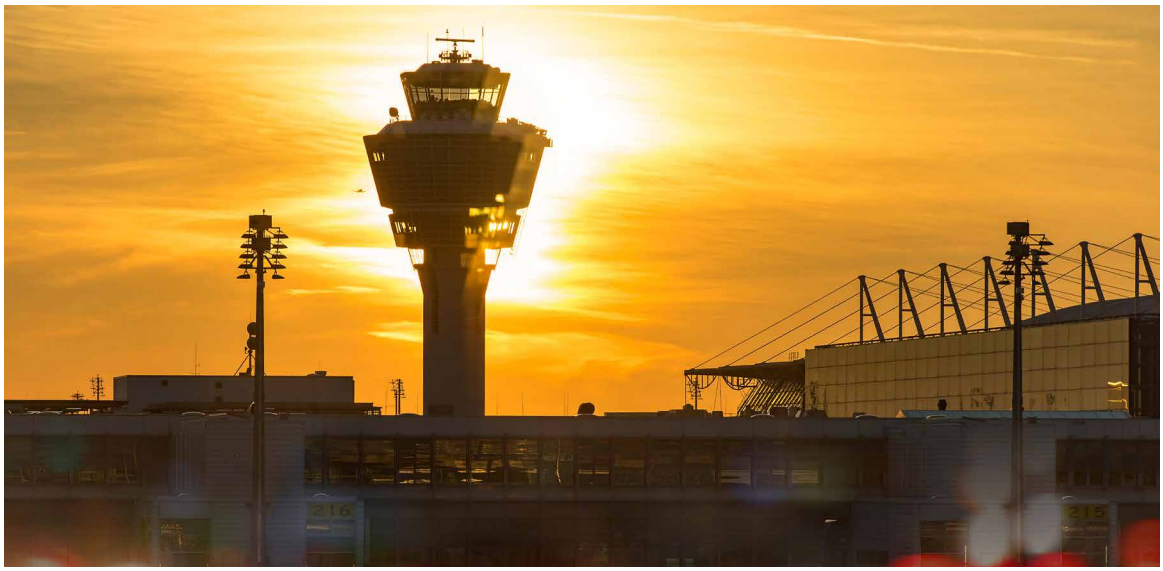
- *S'associer avec les forces de l'ordre et autres autorités publiques :* dans la préparation aux incursions d'UAS hostiles, les exploitants de sites peuvent avoir l'impression que les approches et les techniques pour contrer ce nouveau type de menace leur sont étrangères. Comme ils peuvent effectivement avoir beaucoup à apprendre, il est crucial pour eux de tirer au mieux parti de l'expertise et des conseils que leur offrent les autorités locales, dès le début du processus de planification de la sécurité, pour bien comprendre les risques, les difficultés et les mesures d'atténuation possibles. Des fonds et subventions peuvent aussi leur être accordés par les autorités gouvernementales. Certaines enveloppes ciblent particulièrement la protection anti-UAS, mais il existe aussi des programmes antiterroristes plus généraux qui peuvent englober les mesures de sécurité en lien avec les UAS.

De façon générale, les exploitants de cibles vulnérables ont tout à gagner à s'associer avec les autorités publiques pour déterminer les solutions les mieux adaptées à leur situation, à la lumière de leurs contraintes budgétaires et des cadres juridiques applicables.

Outil 11.
État du contexte de risque mondial de sûreté de l'aviation civile, Doc 10108 – OACI

En 2012, reconnaissant l'importance d'une approche de la sûreté de l'aviation fondée sur les risques, le Groupe de travail sur la menace et les risques du Groupe d'experts de la sûreté de l'aviation (AVSEC) de l'OACI a élaboré la première édition de ce document. L'édition actuelle propose une méthodologie et un cadre destinés à orienter et à soutenir les processus adoptés par les États membres de l'OACI pour assurer la sûreté de l'aviation à l'échelle nationale et locale. On y retrouve également un aperçu des menaces qui pèsent actuellement sur la sûreté de l'aviation dans le monde (dont celles posées par les UAS), ainsi que des évaluations générales des risques à l'échelle mondiale visant à aider les États à élaborer leurs programmes nationaux de sûreté de l'aviation civile. Enfin, l'OACI utilise ce document pour améliorer et mettre à jour les normes et pratiques recommandées de l'Annexe 17 – Sûreté, ainsi que les documents d'orientation.

64 Les exploitants de sites qui souhaitent afficher des panneaux et des avis de mise en garde ailleurs que sur leur site ou sur leur site Web doivent demander la permission aux personnes compétentes.



Le Groupe de travail sur la menace et les risques met le document à jour chaque année et présente au Groupe d'experts AVSEC une analyse et des conseils sur les risques en matière d'aviation. Pour s'acquitter de son mandat, le Groupe de travail s'appuie sur la contribution d'experts, ainsi que sur la communication et le partage efficaces et opportuns d'informations par les États membres de l'OACI.

L'OACI recommande que ce document soit mis à la disposition des responsables des évaluations nationales et autres évaluations des risques pour la sûreté de l'aviation, des décideurs et des professionnels concernés, et des autres parties prenantes. Le document doit être manipulé, communiqué et stocké conformément à la réglementation de chaque État Membre qui s'applique aux informations sensibles en matière de sûreté aérienne.

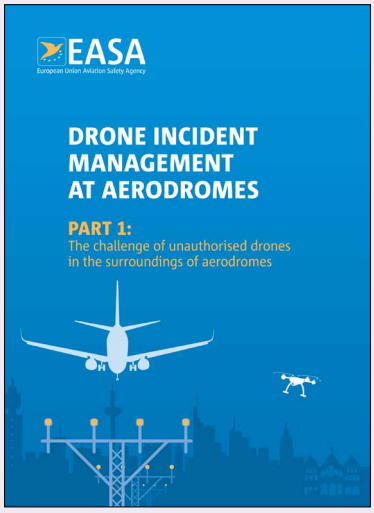
Source : Présentation de M. Sylvain Lefoyer, Directeur adjoint de l'OACI chargé de la sûreté de l'aviation et de la facilitation, lors de la réunion du Groupe d'experts organisée par le Bureau de lutte contre le terrorisme (6 et 7 octobre 2021).

Outil 12.
Drone Incident Management at Aerodromes (Gestion des incidents de drones dans les aérodromes) – Agence européenne de la sécurité aérienne (2021)
(www.easa.europa.eu/drone-incident-management-aerodromes-part-1)

Le guide de l'Agence européenne de la sécurité aérienne (AESA) explique comment mettre en place des mesures et des procédures qui permettront des interventions rapides, efficaces et proportionnelles en cas d'incidents impliquant des UAS. On y recommande essentiellement la mise en place d'un groupe de travail conjoint regroupant les forces de l'ordre, les exploitants aériens et les responsables du contrôle de la circulation

(suite)

aérienne, entre autres, estimant qu'il s'agit là d'une condition préalable à la prise de décisions solides en cas d'urgence. Le document vise également à établir un équilibre entre les possibilités qu'offrent les UAS et les obligations qui incombent aux fabricants et aux exploitants de drones dans les domaines de la sécurité, du respect de la vie privée, de l'environnement, de la protection contre le bruit et de la sécurité publique.



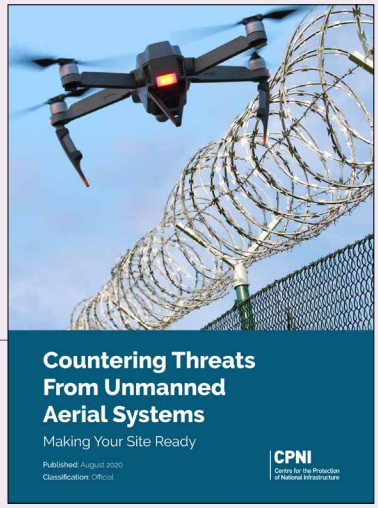
Le guide, qui s'adresse à toutes les entités responsables des questions de sécurité et de sûreté de l'aviation, se divise en trois parties : la première porte sur les problèmes que posent les UAS non autorisés aux abords des aérodromes; la deuxième fournit une orientation et des recommandations; la troisième présente des ressources et des outils pratiques.

Seule la première partie du guide est accessible au public sur le site Web de l'AESA. Pour obtenir la version intégrale, les acteurs du secteur aérien, les agents des forces de l'ordre et les autorités nationales de l'aviation civile peuvent en faire la demande à l'AESA.

Outil 13.
Protecting Against the Threat of Unmanned Aircraft Systems (UAS) : An Interagency Security Committee Best Practice (Protection contre la menace des systèmes de drone aérien : meilleures pratiques) – Département de la sécurité intérieure des États-Unis (2020)
(www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf)

Ce guide des meilleures pratiques décrit des mesures de sensibilisation et d'atténuation que peuvent prendre les professionnels de la sécurité responsables de la protection des sites contre les opérations malveillantes d'UAS. Les sujets suivants y sont abordés : présentation générale des UAS; menaces posées par les UAS; évaluations de la vulnérabilité; mesures et activités de protection; élaboration d'un plan d'intervention en cas d'incident impliquant des UAS; amélioration des connaissances du personnel; mobilisation des partenaires communautaires.

Outil 14.
Countering Threats from Unmanned Aerial Systems: Making Your Site Ready (Contrer les menaces des systèmes de drone aérien : comment préparer votre site) – Centre for the Protection of National Infrastructure (2020)
(www.cpni.gov.uk/system/filesdocuments/40/14/c-uas-branded-doc-public-V4.1.pdf)



Ce guide est un outil d'introduction à l'élaboration d'une stratégie et d'un plan de lutte contre les UAS propres aux sites.

On y retrouve une série de contre-mesures pour atténuer le risque de menaces liées aux UAS, comme des moyens de réduire l'utilisation négligente et imprudente des UAS, des mesures de renforcement physique, une introduction aux solutions techniques disponibles et une démarche pour élaborer une intervention opérationnelle efficace.

3.2.2 Fabricants de systèmes de drone aérien et de sous-systèmes essentiels

Le marché florissant et la demande soutenue d'UAS commerciaux et de loisir incitent les fabricants d'UAS et de sous-systèmes essentiels à améliorer constamment leurs produits pour les rendre de plus en plus puissants et accessibles. Les fabricants d'UAS qui suivent la logique du marché et qui cherchent à surpasser leurs concurrents devraient tirer parti de toutes les innovations technologiques disponibles pour réduire les risques que leurs produits soient exploités par des acteurs hostiles. Actuellement, il semble y avoir deux principaux groupes de mécanismes utilisés à cette fin :

- *Mise en place de capacités de géoblocage :* le géoblocage est une fonction de sécurité de base qui empêche les UAS d'être exploités dans certains espaces aériens (aéroports, établissements pénitentiaires, centrales électriques, etc.) Les logiciels de géoblocage peuvent être mis à jour pour s'adapter au contexte. Par exemple, ils peuvent être configurés de manière à empêcher les drones de survoler le site d'un événement ponctuel très couru. Le géoblocage n'est toutefois pas une solution miracle; il peut manifestement être la cible de pirates informatiques, qui pourraient notamment se servir d'un drone sur mesure pour contourner même la fonctionnalité la plus efficace et la plus difficile à manipuler. Quoi qu'il en soit, le géoblocage peut constituer une première ligne de défense efficace contre les activités malveillantes d'acteurs improvisés ou qui ne disposent pas de cybercapacités pertinentes ou d'un laps de temps suffisant;
- *Transmission des données d'identification des UAS :* les fabricants d'UAS testent une technologie permettant la transmission radio en continu des données d'identification des UAS. À l'instar d'une plaque d'immatriculation, le code d'identification émis par les UAS peut aider le personnel de sécurité et les forces de l'ordre à distinguer les appareils exploités en toute légalité

de ceux utilisés illégalement. Bien que les données transmises ne permettent pas de déterminer si les drones présentent un danger ou non, elles peuvent aider à classer les risques et faciliter la prise de décisions, qui doit souvent se faire dans des délais serrés.

Encadré 13.
Les fabricants de systèmes de drone aérien et les solutions de géoblocage

En 2013, un grand fabricant d'UAS intégrait une fonctionnalité de zones d'exclusion aérienne à ses appareils; trois ans plus tard, il y ajoutait celle de géoblocage, permettant la mise à jour en temps réel et l'ajout de nouvelles zones interdites. Ce système utilise les signaux des satellites de navigation pour éloigner automatiquement les UAS en vol des aéroports, des prisons, des centrales nucléaires, des sites d'événements très médiatisés, etc. À certains endroits, une autorisation spéciale est requise pour que les UAS puissent décoller et voler à l'intérieur d'une zone géobloquée. Les pilotes d'UAS qui possèdent un compte DJI vérifié peuvent débloquer certaines zones s'ils ont des raisons valables de le faire et possèdent les autorisations nécessaires; plus la zone est critique, plus le processus d'approbation est complexe. Les professionnels autorisés à utiliser des UAS dans des endroits vulnérables peuvent soumettre une demande d'autorisation en ligne et recevoir en 30 minutes ou moins un code de déblocage.

Source : www.dji.com/newsroom/news/dji-refines-geofencing-to-enhance-airport-safety-clarify-restrictions.

Cependant, les solutions technologiques de sécurité varient d'un fabricant à l'autre, ce qui risque d'entraîner la création d'environnements cloisonnés, où certaines technologies ne fonctionnent qu'avec des marques ou des modèles particuliers d'UAS. Il est donc clair que les fabricants d'UAS doivent déployer de telles solutions en étroite coordination avec les autorités publiques, mais par-dessus tout avec les autres fabricants afin de garantir que tous adhèrent sérieusement à des normes et protocoles communs et à des approches respectueuses des droits humains.

Les fabricants d'UAS jouent un rôle essentiel à plusieurs égards. Ils empêchent non seulement l'utilisation illégale d'UAS en intégrant dans leurs nouveaux appareils les solutions technologiques les plus avancées, mais ils contribuent également à l'échange de données techniques sur les produits à venir avec les autorités publiques et les organismes de réglementation[65]. En étant informés à l'avance des projets en cours, les autorités seront mieux à même d'anticiper les menaces et d'élaborer des plans d'atténuation et d'urgence plus pertinents, ce qui sera utile tôt ou tard aux exploitants de cibles vulnérables. Parallèlement, les participants à cet échange d'informations privé-public devront recevoir l'assurance que la confidentialité sera adéquatement protégée, quel que soit le canal ou le mécanisme utilisé. Pour être efficace, la circulation des informations doit être assortie d'une garantie que la propriété intellectuelle sera respectée et que les renseignements commerciaux sensibles ne seront pas divulgués de manière à procurer aux concurrents un avantage indu.

Étude de cas 13.
Association des exploitants de drones commerciaux de l'Afrique australe (Commercial Unmanned Aircraft Association of Southern Africa – CUAASA)

La CUAASA a été créée à l'origine pour aider ses membres à bénéficier d'un fondement juridique solide à l'appui de leurs opérations en attendant l'établissement d'un nouveau cadre juridique pour l'exploitation des UAS en Afrique australe. Aujourd'hui, son mandat consiste à servir, défendre, surveiller, promouvoir et protéger mutuellement les intérêts du secteur des UAS commerciaux. Elle compte parmi ses membres diverses entreprises de fabrication et de distribution de haute technologie, des fournisseurs de drones et de services juridiques et une société offrant des cours de pilotage de drones. En plus d'assurer la liaison entre le secteur privé et les organismes publics concernés dans la région de l'Afrique australe, la CUAASA a la responsabilité d'aider ses membres à promouvoir la sécurité, de les préparer au nouveau cadre juridique et d'élever les normes d'exploitation.

En adhérant à la CUAASA, les membres acceptent :

- d'utiliser les UAS de manière légale, éthique et professionnelle et d'obtenir les autorisations pertinentes requises dans l'espace aérien visé, le cas échéant;
- de promouvoir et de favoriser l'expansion du secteur et de la CUAASA;

65 Cette mesure fait partie de celles que les gouvernements sont invités à prendre dans le Mémorandum de Berlin afin de « [m]ettre en place et améliorer la coordination avec le secteur privé et d'autres acteurs non conventionnels » [Bonne pratique nº 14, Forum mondial de lutte contre le terrorisme (2019)].

(suite)

- de signaler les incidents à la police, aux autorités de l'aviation civile ou à l'organisme sectoriel concerné afin d'orienter la croissance du secteur dans la bonne direction.

Ils doivent également adhérer à un code de conduite qui prévoit un ensemble de lignes directrices et de recommandations pour une exploitation sûre et non intrusive des UAS. Ce code de conduite, qui s'articule autour des principes de sécurité, de respect et de professionnalisme, vise à garantir que la vie privée d'autrui et les droits afférents aux autres utilisations de l'espace aérien sont respectés et que les préoccupations du public en ce qui concerne l'utilisation des drones sont prises en compte. Il vise également à fournir aux fabricants et aux utilisateurs une liste de contrôle des opérations et un moyen de démontrer leur engagement envers l'expansion sûre et responsable du secteur.

Source : https://cuaasa.wixsite.com/cuaasa.

Étude de cas 14.
Groupe d'action du secteur des drones (Drone Industry Action Group – Drone IAG) (www.arpas.uk/drone-iag)

Le Drone IAG est un forum multipartite qui rassemble les parties prenantes du secteur des drones du Royaume-Uni dans le but d'établir des liens avec les organismes gouvernementaux, le milieu universitaire, les bureaux de recherche et de technologie, les organismes de réglementation, les investisseurs et les utilisateurs finaux. Il a pour mandat de déceler les tremplins et les écueils qui guettent le secteur et de trouver des moyens d'éviter ces derniers. Ses membres sont censés participer activement à la réalisation de ses principaux objectifs :

- Favoriser l'innovation et la collaboration afin de soutenir l'expansion des applications commerciales de drones ainsi que l'adoption des solutions et des technologies de drones au Royaume-Uni;
- Faciliter l'adoption des UAS dans un large éventail de contextes au sein des secteurs public et privé du pays, ainsi que le suivi et le contrôle des normes appropriées et la contribution à celles-ci;
- Créer des occasions d'adopter des UAS, et faciliter la coordination, la collaboration et l'exploitation de la technologie et d'un système de gestion de la circulation aérienne au Royaume-Uni qui intègre les UAS au reste de l'écosystème aérien;
- Veiller à ce que le secteur soit représenté au sein du Gouvernement et établir un cadre réduisant les utilisations malveillantes des UAS et répondant aux préoccupations de la société;
- Respecter les droits des autres utilisateurs de l'espace aérien;
- Respecter la vie privée d'autrui;
- Tenir compte des préoccupations du public en ce qui concerne l'exploitation des drones.

Le Drone IAG a mis sur pied des groupes de travail qui se penchent actuellement sur les sujets suivants :

- Dossiers de sécurité de l'exploitation – trouver des façons d'améliorer la procédure actuelle d'évaluation des risques de l'autorité de l'aviation civile;
- Espace de conception – proposer des solutions aux défis que présente la mise à l'essai d'applications nouvelles ou complexes;
- Perceptions du public et du monde des affaires – traiter les questions relatives à l'attitude du public et aux façons de mieux faire connaître les services de drones dans les secteurs concernés.

Étude de cas 15.
Détection des vulnérabilités : programme de prime aux bogues

Un important fabricant de drones a instauré un programme de prime aux bogues pour encourager des chercheurs externes spécialisés en sécurité à rechercher activement et à lui signaler les vulnérabilités de ses systèmes et ainsi contribuer à l'amélioration de la sécurité de ses données. Un certain nombre d'exigences doivent être respectées pour participer au programme, notamment : ne pas être à l'origine de la vulnérabilité elle-même, ne pas compromettre de quelque manière que ce soit la sécurité de l'espace aérien public et ne pas utiliser ni exploiter d'une quelconque façon la vulnérabilité pour chercher à découvrir d'autres problèmes de sécurité. Les participants admissibles peuvent recevoir une récompense proportionnelle au risque et à l'incidence estimés de la vulnérabilité signalée.

Source : https://security.dji.com/policy?lang=en_US.

3.2.3 Vendeurs et détaillants de systèmes de drone aérien

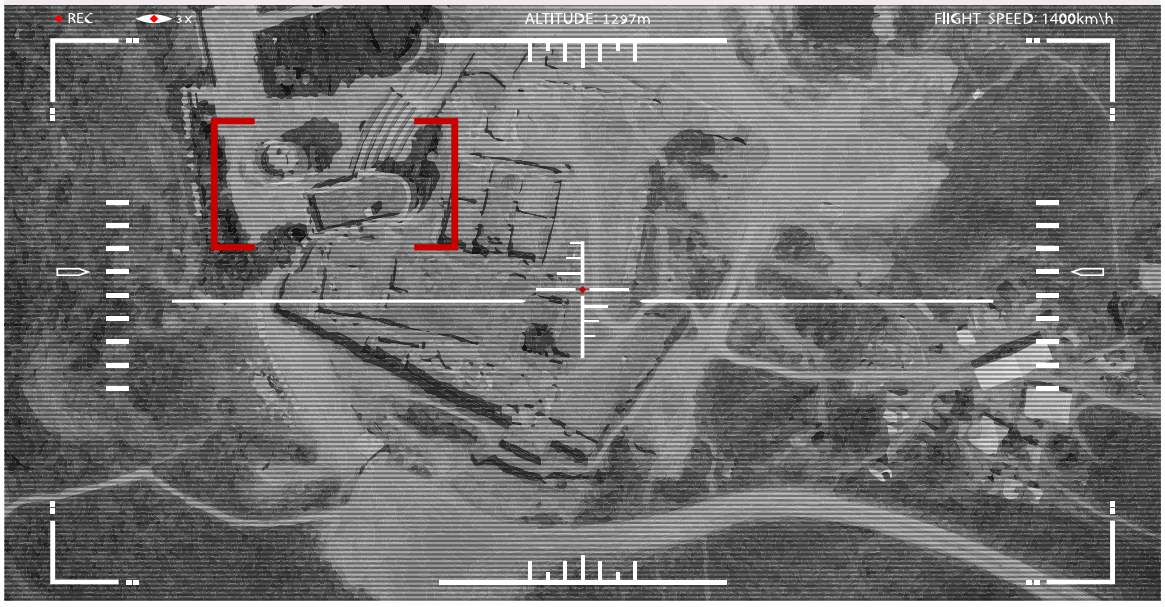
Comme les vendeurs et les détaillants ont un lien étroit avec les clients dans l'écosystème des UAS, ils sont souvent bien placés pour façonner les perceptions des utilisateurs et leur fournir des renseignements clairs et faciles à comprendre sur les questions de sûreté et de sécurité et sur les lois et règlements applicables. Les vendeurs peuvent distribuer et afficher dans leurs magasins et sur leurs sites Web les dépliants, les bannières et les autres documents relatifs à la sécurité officiellement approuvés par le gouvernement, le cas échéant.

Les vendeurs et les détaillants d'UAS peuvent grandement aider à empêcher que les UAS et les équipements connexes se retrouvent entre les mains d'acteurs hostiles. Dans certains pays, ils sont tenus par la loi d'exercer une diligence raisonnable à cet égard, notamment en vérifiant l'identité des clients potentiels et en gardant une trace des transactions réalisées.

Encadré 14.
Signaux d'alarme et manque de diligence dans l'affaire des entreprises IBACS

L'affaire des entreprises IBACS, qui met en cause des UAS achetés par des sociétés affiliées à Daech, démontre comment les entreprises légitimes impliquées dans ces transactions auraient pu éviter de fournir à Daech du matériel en lien avec ces UAS, si elles avaient validé l'identité de leurs clients dès le départ. En effet, les soupçons auraient dû être éveillés immédiatement par les circonstances inhabituelles qui entouraient ces transactions, à savoir :

- La nature des articles achetés (drone, avion télécommandé, composants de fusées, équipement de contre-surveillance);
- Le lieu de destination des articles (près de la frontière du territoire alors contrôlé par Daech);
- Le moment de l'achat (Daech faisait alors les gros titres des médias).



Il est possible d'affirmer que « cette dynamique [...] soulève des questions importantes quant à l'examen interne des achats effectués et aux politiques [...] mises en place par les détaillants pour détecter et prévenir les transactions suspectes, et démontre l'absence apparente de réglementation pour contrôler la distribution de tels composants, en particulier lorsque les articles doivent être livrés à proximité d'une zone de guerre active. La liste des achats effectués par ce réseau met en évidence d'autres problèmes qui auraient dû sonner l'alarme ou déclencher un examen plus approfondi des achats en question, à savoir la quantité d'articles achetés et le nombre de transactions réalisées en un court laps de temps. » À un moment donné, un des conspirateurs a utilisé « des noms différents pour acheter en une seule journée 11 lots identiques de pièces détachées de drones, totalisant plus de 16 000 dollars, pour la même société, à livrer à Şanlıurfa (Turquie) ».

Source : Rassler (2018).

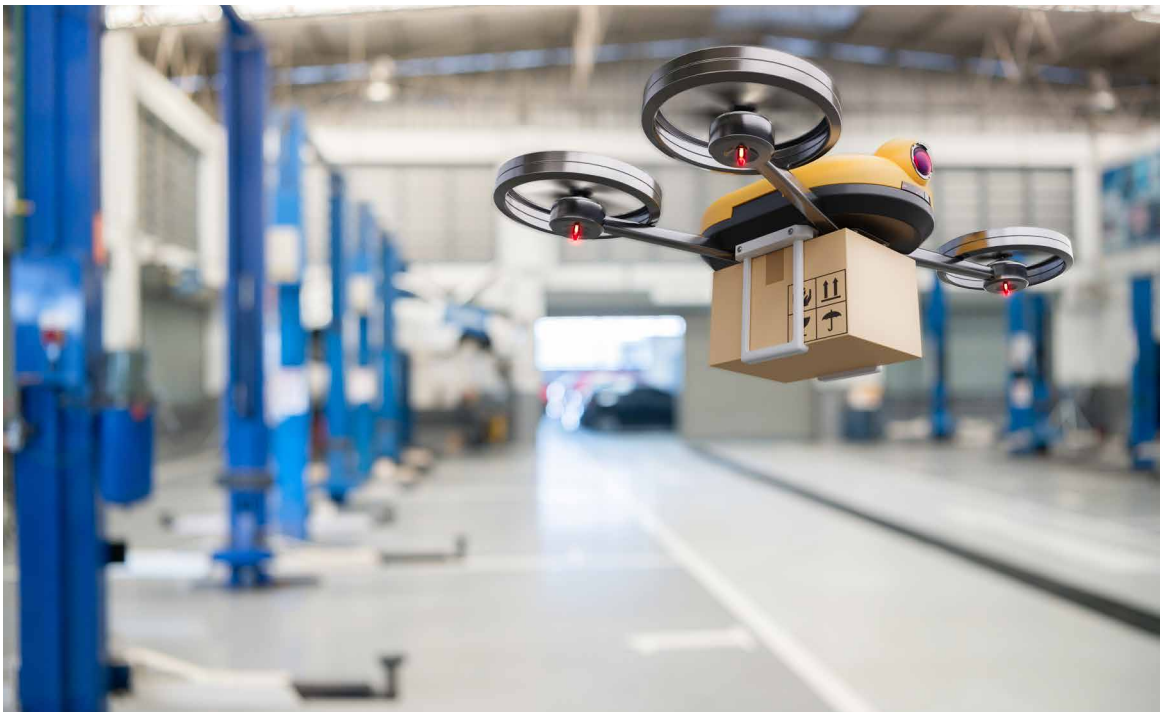
Étude de cas 16. **Programme de certification Dronesafe pour les détaillants du Royaume-Uni**

Lancée en raison de la popularité croissante des drones, cette initiative qui a pris fin en 2021 visait à favoriser une utilisation plus sûre des UAS et à faire savoir au public où, quand et comment les utiliser en toute sécurité. Les utilisateurs étaient encouragés à rechercher le symbole Dronesafe pour s'assurer d'effectuer leurs achats auprès d'un fournisseur responsable et digne de confiance. Pour obtenir la certification Dronesafe, les détaillants devaient répondre aux critères suivants :

- Fournir aux clients une copie du code d'utilisation des drones dans la boîte de tout appareil de plus de 250 g;
- Présenter autrement aux clients, lors de l'achat, une copie du code d'utilisation;
- Afficher bien en vue dans leur magasin le code d'utilisation des drones;
- Donner des conseils clairs aux clients concernant le respect du code;
- Ajouter des liens vers le site dronesafe.uk sur leur boutique en ligne.

Enfin, chaque magasin devait compter parmi son personnel une personne compétente en matière de drones, capable de répondre aux questions des clients et de former ses collègues à cet égard.

Pour participer à cette initiative, les détaillants devaient déclarer qu'ils respectaient les critères ci-dessus auprès de l'Autorité de l'aviation civile. Cette dernière communiquait alors avec eux pour leur confirmer s'ils pouvaient afficher ou non le logo de certification Dronesafe.



3.2.4 Fournisseurs de technologies de lutte contre les systèmes de drone aérien

Les fournisseurs de solutions anti-UAS conçoivent et mettent au point des technologies permettant aux entités autorisées, conformément au cadre juridique national, de détecter, de repérer, de suivre et de neutraliser/intercepter les opérations illégales réalisées au moyen d'UAS. Ces technologies sont activement employées partout dans le monde pour protéger les cibles vulnérables. Par exemple, lors de la Coupe du monde 2018 de la FIFA, organisée en Fédération de Russie, les autorités et les forces de sécurité ont déployé des systèmes anti-UAS dans les stades pour repousser les attaques potentielles de drones. Un autre système anti-UAS a été installé pour protéger les infrastructures et les dignitaires lors du sommet du G20 tenu à Buenos Aires en 2018[66].

Il est essentiel que les fournisseurs de solutions anti-UAS établissent des liens de communication très étroits avec les organismes gouvernementaux et les forces de l'ordre, qui sont les utilisateurs finaux. La collaboration est primordiale pour s'assurer que les solutions sont élaborées dans le respect des droits humains et que les parties prenantes du secteur demeurent au fait des fondements juridiques en constante évolution et mettent au point ou adaptent constamment leurs technologies pour répondre aux menaces nouvelles et naissantes liées aux UAS.

3.2.5 Utilisateurs de systèmes de drone aérien

Le nombre d'utilisateurs finaux des produits et services liés aux UAS augmente de façon exponentielle à mesure que de nouvelles personnes, entreprises et organisations adoptent cette technologie à des fins récréatives, commerciales ou professionnelles[67]. Dans tous les cas, il incombe aux exploitants d'UAS d'utiliser

66 Ce système comprenait un radar 3D en bande X pour détecter les objets potentiellement menaçants, une caméra optoélectronique/infrarouge pour les classifier et un brouilleur pour les neutraliser.

67 Entrent notamment dans cette catégorie les entités qui possèdent une flotte d'UAS utilisée pour réaliser les projets de leurs clients, mettant ainsi en place un nouveau modèle d'affaires appelé « services d'UAS à la demande » (voir encadré 15).

leurs appareils en respectant pleinement leurs obligations légales et les normes de sûreté et de sécurité en vigueur. Ils doivent notamment les enregistrer, obtenir les permis nécessaires et se soumettre aux examens requis.

Il y a donc collaboration entre, d'une part, les exploitants d'UAS qui, en se conformant aux exigences, réduisent les risques de compromettre la sécurité des personnes et des installations et de voir leur responsabilité personnelle engagée et, de l'autre, une communauté d'utilisateurs finaux qui, en se montrant responsables, permettent de diminuer les cas d'utilisation négligente des UAS dans l'espace aérien réglementé. Les forces de l'ordre et le personnel de sécurité (notamment les responsables de la protection des sites vulnérables) peuvent ainsi mieux mettre à profit leurs capacités de détection et leurs ressources limitées, vu l'éventail plus restreint d'événements potentiellement menaçants impliquant des UAS.

Les utilisateurs peuvent également réduire considérablement le risque de voir leurs propres appareils détournés ou autrement piratés. Dans bien des cas, la principale façon de gérer ce risque consiste à respecter les normes de base en matière de cybersécurité, comme mettre régulièrement à jour les logiciels des UAS, choisir des mots de passe robustes, s'assurer que les dispositifs de contrôle au sol (y compris les smartphones et les ordinateurs portables) sont protégés contre les logiciels malveillants, et utiliser un réseau privé virtuel (VPN) pour empêcher les pirates d'accéder aux connexions Internet[68]. De plus, les utilisateurs qui possèdent un UAS muni d'un mode « Retour au point de départ » seront en mesure de récupérer leur appareil en cas de détournement, puisque ce dernier reviendra automatiquement à son point de départ s'il perd le signal ou si ce dernier est brouillé[69] [Kaspersky (2021)].

68 Un VPN agit comme une passerelle sécurisée vers Internet et permet de chiffrer la connexion.

69 Comme le fonctionnement du mode « Retour au point de départ » dépend du GPS, cette fonctionnalité peut ne pas fonctionner en cas d'une usurpation GPS, c'est-à-dire si les signaux GPS sont brouillés pour faire croire que l'appareil se trouve ailleurs.

Encadré 15.
Services de systèmes de drone aérien à la demande

Ces dernières années, des organismes gouvernementaux ont commencé à faire appel à des entreprises privées pour qu'elles déploient leurs UAS sophistiqués dans le cadre d'opérations de surveillance et de contrôle. Le concept des services d'UAS à la demande représente un nouvel aspect des partenariats public-privé dans l'écosystème des UAS. Lorsqu'il repose sur un cadre juridique mettant en avant de solides principes éthiques et légaux, il permet aux gouvernements de se concentrer sur les résultats plutôt que sur les ressources, d'utiliser la solution la plus appropriée pour chaque cas et d'adopter des cadres contractuels flexibles qui reflètent la souplesse opérationnelle de ce service[70].

Ce concept peut être particulièrement intéressant pour les services de police qui ne disposent pas de technologies d'UAS suffisamment avancées ou de l'expertise technique nécessaire pour bien s'en servir, de même que pour les pays qui, en raison de leurs ressources financières limitées, ne pourraient pas se procurer leur propre flotte d'UAS ni en supporter les coûts d'exploitation.

3.2.6 Utilisateurs de cibles vulnérables

Grâce aux conseils clairs et simples que les forces de l'ordre et le personnel de sécurité leur fournissent, les visiteurs de sites touristiques et de lieux emblématiques, les spectateurs d'événements en plein air, etc. peuvent jouer un rôle important dans la gestion des menaces provenant des UAS qui pèsent sur les sites vulnérables. Il est possible, par exemple, que certains de ces sites ne disposent pas de technologies anti-UAS permettant de détecter les UAS menaçants, ou que leurs solutions technologiques s'avèrent insuffisantes ou peu efficaces selon l'éclairage ou les conditions météorologiques. Dans tous les cas, la capacité générale du public à repérer et à signaler les situations inquiétantes peut constituer un élément essentiel dans un environnement de sécurité à plusieurs niveaux.

3.2.7 Organisations de la société civile

Les organisations de la société civile peuvent tirer parti de leur position en améliorant les liens entre le public et les autorités compétentes à l'égard des questions de sûreté et de sécurité des drones. Par exemple, elles peuvent servir d'intermédiaires en veillant à ce que le public soit informé des cadres réglementaires et des politiques publiques qui traitent des menaces liées aux drones et de leur prévention. En outre, les organisations locales indépendantes peuvent aider à formuler efficacement les préoccupations et les idées de la société civile et à les transmettre aux décideurs, aux organismes de réglementation et aux forces de l'ordre. La contribution des organisations de la société civile peut être sollicitée à différentes étapes des processus d'élaboration des politiques et des lois, y compris lors de l'analyse coût-bénéfice et de l'évaluation des risques, de la phase de rédaction et de la communication des règles.

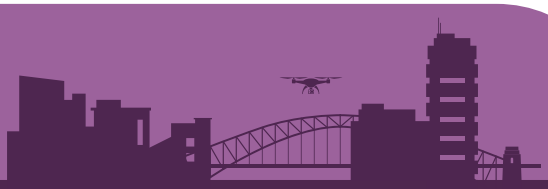
70 Par exemple, le modèle des services d'UAS à la demande a été utilisé par le Ministère de l'intérieur du Royaume-Uni comme outil clé pour aider à prévenir la migration illégale et la pêche illicite.

Au-delà des communications, les organisations de la société civile peuvent contribuer substantiellement aux efforts de relèvement et aider les victimes d'un attentat terroriste impliquant un drone à faire valoir leurs droits. Certaines organisations non gouvernementales utilisent activement les UAS pour soutenir les interventions en cas de crise, que l'incident implique ou non des UAS (voir étude de cas 17).

Étude de cas 17.
Drones Sans Frontières
(www.droneswithoutborders.org)

Fondée en 2019, Drones Sans Frontières est une organisation non gouvernementale qui a pour mission d'exploiter la technologie des UAS afin de fournir une capacité de surveillance technique et des informations en temps réel aux intervenants en cas d'urgence et de catastrophe ainsi qu'aux autres partenaires sur le terrain en réponse aux crises, que celles-ci soient d'origine naturelle ou humaine.

Réalisant sa mission sous les trois pôles opérationnels que sont l'évaluation de l'impact, la vérification des besoins et la promotion de l'aide humanitaire, Drones Sans Frontières contribue à la gestion des crises et aux efforts de relèvement en mettant l'accent sur les personnes vulnérables touchées par les situations d'urgence.



Références

Association of the United States Army (2021). *The Role of Drones in Future Terrorist Attacks* (www.ausa.org/publications/role-drones-future-terrorist-attacks).

Canada, Ministère des transports (Transports Canada) (2021). *Stratégie de Transports Canada en matière de drones à l'horizon 2025* (https://tc.canada.ca/fr/aviation/publications/strategie-transports-canada-matiere-drones-horizon-2025).

États-Unis d'Amérique, Département de la défense (2021). *Counter-Small Unmanned Aircraft Systems Strategy* (https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf).

Europol (2021). *European Union Terrorism Situation and Trend Report* (www.europol.europa.eu/tesat-report).

Forum mondial de lutte contre le terrorisme (2019). *Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités* (www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20FR.pdf?ver=2020-01-13-143548-203).

Kaspersky (2021). « Sécurité et drones : ce que vous devez savoir » (www.kaspersky.fr/resource-center/threats/can-drones-be-hacked).

Ley Best, Katharina *et al.* (2020). *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools*, RAND Corporation (www.rand.org/pubs/research_reports/RR2972.html).

Ministère de l'intérieur du Royaume-Uni (2018). *Stop and Search: Extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers and corrosive substances: Government consultation* (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739629/06_09_18_Stop_and_Search_Consultation_Document_.pdf).

_____ (2019). *UK Counter-Unmanned Aircraft Strategy* (www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy).

Moore, Jack (2016). « Rio Olympics: Al-Qaeda Jihadis Call for Attacks on American, British, French and Israeli Athletes », *Newsweek*, 22 juillet 2016 (www.newsweek.com/al-qaeda-jihadis-call-attacks-american-british-french-israeli-athletes-rio-483145).

Organisation des Nations Unies, Conseil de sécurité, Rapport final du Groupe d'experts sur la Libye créé par la résolution 1973 (2011), 8 mars 2021 (www.un.org/securitycouncil/sanctions/1970/panel-experts/reports)

Palestini, Claudio (2020). « Lutte contre les drones : à la recherche de la solution miracle », *Revue de l'OTAN* (www.nato.int/docu/review/fr/articles/2020/12/16/lutte-contre-les-drones-a-la-recherche-de-la-solution-miracle/index.html).

Rassler, Don (2016). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology, Combating Terrorism Center at West Point* (www.jstor.org/stable/resrep05632).

_____ (2018). *The Islamic State and Drones: Supply, Scale, and Future Threats, Combating Terrorism Centre at West Point* (https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf).

Staniforth, Andrew (2017). « Attack of the drones – Emerging threats from Unmanned Aerial Vehicles », TRENDS Research & Advisory (https://trendsresearch.org/insight/attack-of-the-drones-emerging-threats-from-unmanned-aerial-vehicles).

Pour en savoir plus, voir :

www.un.org/counterterrorism/vulnerable-targets

2118451-5

NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME