Version préliminaire

Table des matières

Élaboré par le Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables du Bureau de lutte contre le terrorisme (BLT)[1], le présent document se veut une source d'orientation concernant la protection des cibles vulnérables contre les attaques terroristes impliquant des systèmes de drones aériens (UAS). Il s'agit d'un module sectoriel du 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 UAS, suivi d'une brève explication des indications croissantes de l'intention des terroristes d'utiliser les UAS pour mener des attaques, le présent module traite du rôle précis que chaque partie prenante peut et doit jouer dans un environnement de sécurité complexe – et

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 le3-tures critiques du PNations Unies de coordination contre le terrorisme

Des renseignements im
d'experts organisées pa
nisations et égionales, s
sitaire.(le3)0.La premièr

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

Les UAS comprennent divers modes de navigation aérienne[6], qui les rendent autonomes

Les UAS continuent de bénéficier d'un essor technologique[7] et des avancées théoriques et pratiques en intelligence artificielle (IA)[8]. En outre, de nombreux UAS vendus sans restriction peuvent être facilement modifés ou améliorés pour répondre aux 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 nou-

Au cours des dernières années, les forces de l'ordre ont détecté ou contrecarré divers plans liés au terrorisme qui reposaient sur l'utilisation d'UAS dans des zones exemptes de conflits[11]. 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 en utilisant différents vecteurs d'attaque, dont des UAS chargés d'explosifs. 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 pos-

Encadré 1.

CL AC OSC NM CLR C WR C BC BRM LC PGL CR C ECLR

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[17].

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 la 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 d'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.

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 (périmètres des sites renforcés afin de freiner les attaques en voiture, gardes armés, barrières pour le contrôle des visiteurs, etc.). En outre, de nombreux modèles d'UAS faciles à utiliser peuvent être achetés à peu de frais, ce qui constitue une incitation supplémentaire pour les groupes terroristes ou les acteurs isolés qui cherchent de nouveaux moyens peu coûteux de réaliser leurs activités.

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 des 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].

17 Pour une analyse générale des problèmes avec lesquels les acteurs non étatiques peuvent être appelés à composer 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, à l'adresse : https://www.middlebury.edu/institute/news/UAS-and-cbrn-terrorism-threats-and-responses (en anglais seulement).

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 réussir à faire plus de victimes (Don Rassler, réunion du Groupe d'experts organisée par le BLT les 6 et 7 octobre 2021).

Les groupes terroristes peuvent avoir recours à des UAS pour atteindre différents objectifs[20]. Ils peuvent notamment les utiliser contre des cibles vulnérables aux fns 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 l'encadré 1). Leurs signaux de communication peuvent aussi servir, par exemple, à activer des brouilleurs de fréquences radio pour interférer avec les

20 Voir le texte d'orientation technique concernant la résolution 2370 du Conseil de sécurité, sous-module II, section 1.1.2 sur l'utilisation des UAS à des fns terroristes.

21 En août 2018, le Président vénézuélien Maduro a été la cible d'une tentative d'assassinat ratée 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 de petites bombes de la taille d'un caillou. Bien que l'utilisation de ces appareils n'ait pas changé l'issue du conflit, elle a mis en évidence les conséquences potentiellement mortelles que peuvent avoir les 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 russes en Syrie ont été attaquées par une flotte de 13 UAS

- **h LDMP RGML x** 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;
- **h CLG MD CPTGAC x B LGBC CPTGAC** Par exemple, pirater les logiciels de contrôle de drones pour que les appareils ne répondent plus aux commandes du pilote;
- **h CT RGML MDNPGTGCEC x T RGML BC NPGTG EC** Violation du principe d'autorisation à exécuter une action donnée; par exemple, détourner un UAS en se faisant

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. » (Forum mondial de lutte contre le terrorisme, 2019, bonne pratique n° 5)

Encadré 3.
4SLP GGR BL GLDP RPSARSRC GLDMP RGDSC BC WR C BC BRMLC RGCL

L'infrastructure informatique mise en place par les fabricants d'UAS 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 d'UAS 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 inf ƙ p m γ v φ l ᵀW m ᵇ ᴰent א aut desautilicateurnn

ACBCSP

Les organismes gouvernementaux ont le devoir de mettre en place un cadre général visant à faciliter : i) la prévention et la gestion des incidents impliquant des UAS; ii) un retour à la normale rapide et du soutien pour les sites et personnes affectés.

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 pour protéger les sites vulnérables exposés aux attaques terroristes en général, tout en assurant la promotion et la protection des 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 four

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

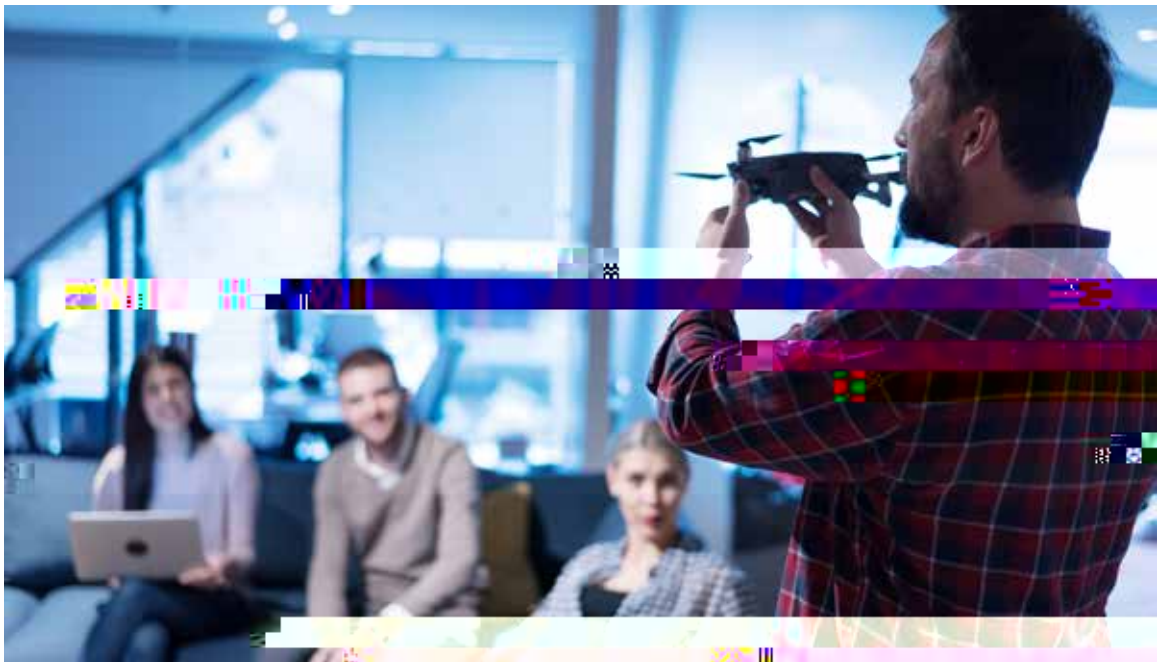
Sur le plan procédural, les pays qui entreprennent d'élaborer une stratégie de lutte contre les UAS devraient mener une consultation pangouvernementale qui permettra de produire un document stratégique ciblé et complet.

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 [d'UAS] par des acteurs violents non étatiques dans le cadre de con f its armés[29] » (Forum mondial de lutte contre le terrorisme, 2019, bonne pratique nº 11);
- 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 d'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

28 La stratégie du 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 dé f nir les priorités politiques à respecter d'ici 2025 (Canada, 2021).

29 Le Mémorandum de Berlin précise toutefois tout e'Oa er ånngτ D ä ⌄ " e prirft d Ǝ r ä ʌ τ érft τ' ċ Ɪ r



peuvent prendre la forme, entre autres, de projets de recherche et développement visant l'introduction ou l'amélioration de fonctions de sécurité, ainsi que de discussions soutenues sur l'incidence que les technologies déployées dans les nouveaux modèles peuvent avoir dans le contexte de la sécurité.

Encadré 4.
1PP R EGCN LEMSTCRLC CLR CRCAM LB CN P - NMSP C WR C BCBRMLC RGL

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 planifer 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'in-

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

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 e f caces.

Cette stratégie a été élaborée à titre de complément à CONTEST, la stratégie britannique antiterroriste, ainsi qu'à la stratégie de lutte contre les crimes graves et la criminalité organisée du pays.

Source : Royaume-Uni, 2019.

Étude de cas 3.
NNRMAFCBC1GLE NMSPD AC SVPGOSC BC ASRGR NM NPC WR C BCBRMLC PGL

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 où beaucoup de gens se rassemblent. En outre, en juin 2019, la présence d'UAS autour de l'aéroport de Singapour Changi a contraint les autorités à restreindre temporairement les opérations sur les pistes, ce qui a causé des retards et forcé le détournement de certains vols.

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

- **PEC CLRRGML** Le Parlement de Singapour a adopté son projet de loi sur les drones aériens (sûreté et sécurité publiques) en 2015 a f n de réglementer l'exploitation des drones, et son projet de loi sur la navigation aérienne (modi f cation) 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 : i) certains vols de drones

Encadré 5.

Les systèmes de gestion du trafc aérien existants sont mal équipés pour faire face à l'augmentation du trafc généré par les UAS de toutes sortes et pour encadrer leurs profls de vol. C'est pourquoi i ʁ q ʊ M m l M

Étude de cas 5.

BPC BC EC RGML BC PG OSC BC OP R P C SLG AML ACRL LR C PML CD LML SRMPG B L C N AC PGL AML PP

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 afn de déterminer les te

BSA RBVL CR CL GGG RBVL

Les utilisateurs fnaux d'UAS, en particulier des 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 leur vulgarisant les cadres de réglementation en matière de sûreté et de sécurité qui s'avèrent, dans bien des cas, complexes et très techniques.

39 Les gouvernements peuvent également envisager d'utiliser les médias et les publications consacrées aux drones afn de

Outil 6.
M SLCA RGML TCA CVR RGCSP GLDMP RGML CR CL G GG RGML RRMS CBMSRG BC - R
(https://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 [ou la] télépilote doit accepter la responsabilité et comprendre qu'il

Campagnes de sécurité :
Il peut se révéler e f cace 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 facilitent l'appréciation de la Mא on Ӈ΄ϒ ί ŝ

•gsucc et0ivlocaux uberiqLatgesa2-n /G /GS100c /G06500490003>]TJ /TTti9.ss expldn2es e8/Sri5 sss expleter

•

- 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.) (Forum mondial de lutte contre le terrorisme, bonne pratique nº 8);
- La mise en place de mécanismes permettant aux autorités nationales d'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[41];
- 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 et développement, notamment le partage des résultats et l'identification de possibilités de collaboration sur des projets futurs et en particulier, la gestion v

  les ex351cd'U

  –

41 Vu l'absence d'une norme de classification douanière particulière pour les UAS, les fabricants d'UAS légitimes sont tenus d'utiliser actuellement 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.

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 territoire à partir duquel un drone est exploité, par exemple, peut devoir traiter rapidement une demande lui pro04C2 (v)7.4.1 ation.

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 e f cacement 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 dans les 0AB005500441 Tf0.049 Tw 0 -1.4;[(lage ommeTj0.3 49 Tw 0 -nuit,v)7.4 (o)6.4 (ecad(AS 6ampleur dgo

- Il convient de s'assurer que les opérations de surveillance par UAS ne sont pas in-

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 menées après coup 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 des enquêtes 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 d'emblée à leurs supérieurs. En outre, les enquêtes et les personnes qui les mènent doivent être indépendantes de toute influence indue et doivent être 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 convenablement les

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, si jamais des UAS armés parvenaient à contourner les mesures de sécurité du site vulnérable. 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, sous la supervision des policiers et du personnel du site chargé de la sécurité, la tenue d'exercices d'évacuation réguliers qui simulent des scénarios de crise précis afn 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 afn 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 e f cacement s'ils acquièrent les connaissances requises avant qu'une crise n'éclate.

Encadré 8.

LR EP RGVL BC CLDVP RGVL PCASCGGC GBC BC WR C BC BRVLC RGCL B L CRPT GBC ACLRPC BC ACLRP G RGVL BS PCL CGELC CLR

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 sur la lutte antiterroriste. Les capacités de renseigne-

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'UE. Les informations obtenues au moyen des UAS peuvent contribuer à s'acquitter de cette responsabilité.

Toutefois, le piratage d'UAS est un risque dont il faut tenir compte. Comme les UAS feraient partie du réseau de transmission de renseignements aux centres, ils 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'aqgicielsiicdTw 0 -1.4 Td[(obtenui

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 person

Étude de cas 10.

GC C GCR T S RGML BC AMLRFC C SRC TG LR C BRMLC SL CVCPAGAC B , 2 0. - CRBC NMGAC LMPT EGLLC

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 afn d'assurer la sécurité d'un environnement aéroportuaire par la détection, le suivi et la reconnaissance des drones, ainsi que l'identifcation de leurs pilotes[50].

Chaque contre-mesure a été évaluée et notée en fonction de critères précis. Les conclusions pourront ainsi être rassemblées pour 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 ex-

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 : https://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, lors de la réunion du Groupe d'experts organisée par le BLT (6 et 7 octobre 2021).

Étude de cas 11.

3RGG RGML BC WR C BCBRMLC RGL N P NMGACBC R MELC

Lors du congrès mondial de la téléphonie mobile tenu à Barcelone en 2018, le service de police autonome (« Mossos

Bade(cep3.o 0 0[(BaS0 03.81)9.5c[(Ba979et -1.4 Td369J0.318 Tw -10.9 0.913o)73fj7519.4l 6.831 -1.6/2

Outil 7.

M LLC NP RGDSC CR C SPC BC ASPGR MP BS B NMGC CLR BCRCAFLMMEGC BC SRRC AMLRPC C WR C BCBRMLC RGCL GLGR RC BC RP L NMRR BS 0MW S C 3LG

[( )T7g927ys d5

équitable. De même, les enquêtes qui impliquent des UAS présentent leur lot de particularités et de difficultés. Il est important que les forces de l'ordre comprennent ces particularités 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 UAS 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

52 Voir le sous-module II du texte d'orientation technique concernant la résolution 2370, 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).

Étude de cas 12.

. MSTMGPBGLRCFNC RGML CRBCDMSGC E RB BC WR C BCBRMLC RGCL

En 2018, le Ministère de l'intérieur britannique 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 à l'Air Navigation Order 2016 (décret sur la navigation aérienne 2016). La police a en main une description de l'individu et de l'endroit. Les agents ont patrouillé dans le secteur à l'heure où la plupart des appels concernant l'incident ont été reçus et identifent 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'en 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

Outil 10.
Cadre d'intervention en cas d'incident lié à un drone : À l'intention des

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 la e, e4 acpouv f2P2

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,

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.

VN MGR LR BC AG C TS L P C

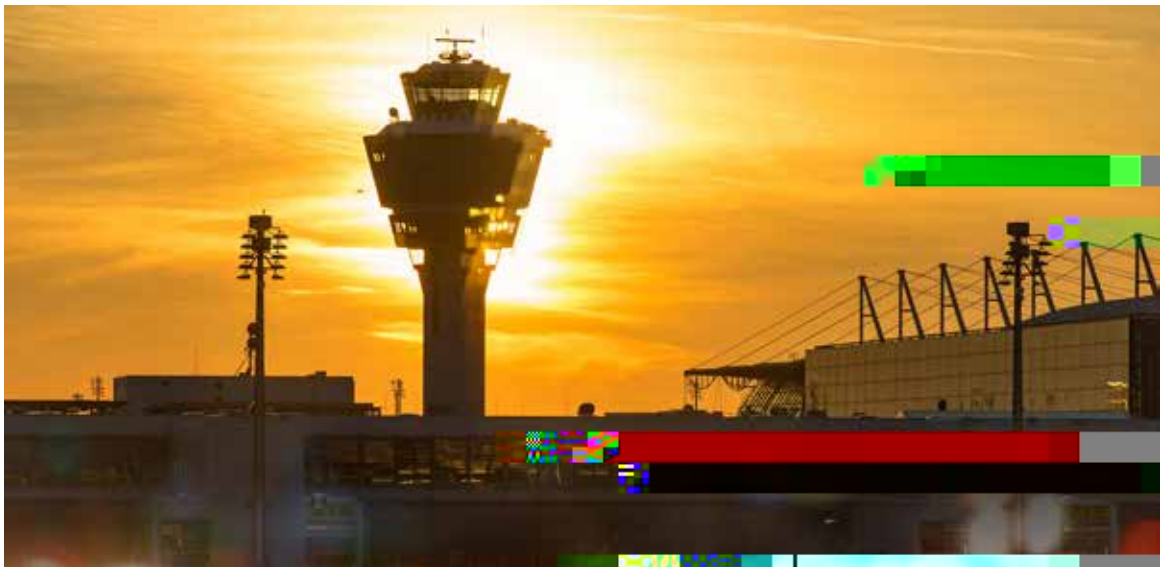
Les propriétaires et aux gestionnaires de sites vulnérables qui souhaitent protéger leur site contre le risque d'activités terroristes impliquant des UAS peuvent prendre diverses mesures importantes.

- Inclur

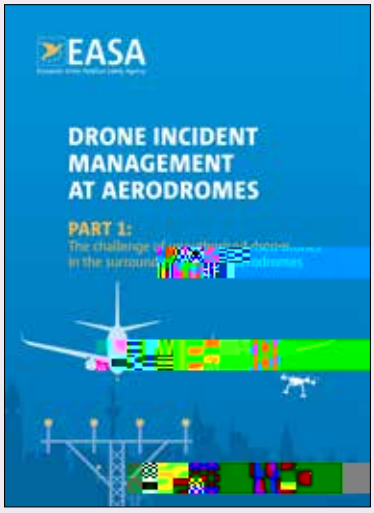
60 Les menaces liées aux UAS ne sont pas forcément statiques; elles sont potentiellement dynamiques, et les plans de gestion des crises doivent en tenir compte. Par exemple, un drone peut se poser à un endroit vulnérable du site pour se diriger l'instant d'après vers un autre point de vulnérabilité. 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.

comptes de médias sociaux peuvent



les forces de l'ordre, les exploitants aériens et les responsables du contrôle de la circulation aérienne, entre autres, estimant qu'il s'agit là d'une condition préalable à la prise de décisions réfléchies 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 au chapitre 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 . RMRCARGML AMLRPC CL AC BC WR C BC BRMLC PGCL C CG CSPC NP RGDSC LRCP ECLAWI CASPGW M GRCC BC R R 3LG
[https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf (en anglais seulement)]

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'incidents impliquant des UAS; amélioration des connaissances du personnel; mobilisation des partenaires communautaires.

Outil 14.
Countering Threats from Unmanned Aerial Systems: Making Your Site Ready ML RFCP C CL AC BC WR C BC BRML C PGCL AM CLRNP N RCPTMRFC GBC CLRFC DMPRFC. RMRCARBML MD, RBML LDP RPSARSRC BS 0MW S C 3LG
[https://www.cpni.gov.uk/system/ fles/documents/40/14/c-uas-branded-doc-public-V4.1.pdf (en anglais seulement)]

Ce guide, qui se veut un outil d'introduction à l'élaboration d'une stratégie et d'un plan de lutte contre les UAS adaptés au site du lecteur, s'adresse aux responsables de la protection des infrastructures nationales, des sites vulnérables et des lieux très fréquentés, notamment à ceux chargés de la sécurité des sites, de la sécurité physique, des salles de contrôle de sécurité et de la continuité des activités.

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 e f cace.

PGA LR BC WR C BC BRML C PGCL CRBC MS WR C C CLRGC

Le marché forissant 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 fn :

- 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 confgurés 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 cont { z z تذ

- 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 UAS exploités en toute légalité de ceux utilisés illégalement. Bien que les données transmises ne permettent pas de déterminer si les drones sont inoffensifs ou menaçants, elles peuvent aider à classer les risques et faciliter la prise de décisions, qui doit souvent se faire dans des délais serrés.

Encadré 13.
C D PGA LR BC WR C BC BRMLC PGGL
CR C MSRGML BC E M MA EC

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 zzBien Ctèmes de intsése0.024 Tw0 -1.4 Td[(ellesolutiign (

Cependant, les solutions de sécurité technologiques 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 a f n 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

65 Cette mesure fait partie de celles utte ¿ celle ec

(suite)

- de signaler les incidents à la police, aux autorités de l'aviation civile ou à l'organisme sectoriel concerné afn 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 la sécurité, du respect et du 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 (en anglais seulement).

Étude de cas 14.
RMSNC B ARQML BS CARCSPBC BRMLC RMLC LBS RPW ARQML RMSN

[https://www.arpas.uk/drone-iag/ (en anglais seulement)]

Le DIAG est un forum multipartite qui rassemble les parties prenantes du secteur des drones 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 fnaux. 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 afn 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 sec-

4CLBCSP CRB R G LR

MSRLG CSP BC RCAFLMMEGC BC SRRC AMLRRC C WR C BC BRMLC PGCL

Les fournisseurs de solutions anti-UAS conçoivent et mettent au point des technologies permettant de détecter, de repérer, de suivre et de neutraliser/intercepter les opérations illégales réalisées au moyen d'UAS. Ces solutions sont créées à l'intention des entités autorisées, conformément à chaque cadre juridique national. Elles sont activement employées partout dans le monde pour protéger les cibles vulnérables. Par exemple, Lors de la Coupe du monde 2018 de la FIFA en 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 de Buenos Aires en 2018[66].

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

67 Entrent notamment dans cette catégorie les entités qui possèdent une fotte d'UAS utilisée pour réaliser les projets de leurs

Encadré 15.

concernant les principales préoccupations soulevées, notamment à propos du renforcement des droits humains. 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.

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 des UAS à faire valoir leurs droits. Certaines organisations utilisent activement les UAS pour soutenir les interventions en cas de crise, que l'incident implique ou non des UAS (voir l'étude de cas 17).

Étude de cas 17.
PMLC 1 L PMLRGPC
[https://www.droneswithoutborders.org/ (en anglais seulement)]

Fondée en 2019, Drones Sans Frontières est une organisation non gouvernementale qui a pour mission d'exploiter la technologie des UAS afn de fournir une capacité de

Association of the United States Army. The Role of Drones in Future Terrorist Attacks, 2021
(

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

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

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

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

Royaume-Uni. Counter-Unmanned Aircraft Strategy, 2019 (https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy).

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