Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités

Introduction

Les systèmes d'aéronefs non habités (UAS, *Unmanned Aerial Systems*)[1] relèvent d'une technologie qui évolue très vite. Les systèmes d'aéronefs non habités sont utilisés (et le seront encore plus à l'avenir) pour des activités importantes, positives et légitimes, aussi bien par les gouvernements (par exemple lors d'interventions d'urgence en cas de catastrophe ou de lutte contre les incendies) que par le secteur privé (par exemple, pour des usages agricoles, la surveillance d'oléoducs, la livraison de biens de consommation). Néanmoins, les observateurs avertis craignent que les terroristes continuent eux aussi à utiliser les systèmes d'aéronefs non habités pour la poursuite de leurs propres objectifs illicites et illégaux. Les utilisations malveillantes des systèmes d'aéronefs non habités ne se limitent pas aux attaques physiques mais recouvrent également des opérations de collecte de renseignement, de surveillance et de reconnaissance ; l'observation de cibles, de protocoles de sécurité et de structures de comportement ; les exploitations visant à améliorer la précision des tirs indirects ; l'enregistrement de séquences vidéo à des fins de propagande terroriste ; la perturbation des opérations des forces de maintien de l'ordre ; la perturbation, l'intrusion malveillante et la paralysie d'infrastructures clés, du trafic aérien et d'actifs économiques ; la contrebande de marchandises illicites, transfrontalière ou destinée à des zones sensibles ; l'intimidation ou le harcèlement ; le déclenchement de mouvements de panique lors de rassemblements de foule. Les attentats terroristes commis au moyen de systèmes d'aéronefs non habités peuvent viser diverses cibles gouvernementales, économiques et toute autre infrastructure critique, ainsi que des cibles publiques (plus généralement désignées « cibles civiles »)[2]. Le risque que des systèmes d'aéronefs non habités puissent être utilisés lors de cyberattaques ou en tant que vecteurs chargés d'explosifs ou d'agents chimiques, biologiques ou radiologiques est également une source croissante d'inquiétude. En vertu de la Résolution 1540 (2004) du Conseil de sécurité des Nations Unies (RCSNU 1540), tous les États sont tenus d'adopter et d'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. La RCSNU 1540 impose également aux États de prendre et d'appliquer des mesures efficaces afin de mettre en place des dispositifs internes de contrôle destinés à prévenir la prolifération d'armes nucléaires, chimiques ou biologiques ou de leurs vecteurs. Dans la mesure où les systèmes d'aéronefs non habités constituent des vecteurs dans le sens spécifié ci-dessus, le

[1] Dans sa Circulaire 328-AN/190, *Unmanned Aircraft Systems (UAS)* [*Systèmes d'aéronef sans pilote (UAS)*], l'Organisation de l'aviation civile internationale (OACI) propose de définir un UAS comme un « aéronef et ses éléments reliés qui sont manœuvrés sans pilote à bord ». Par conséquent, le terme *Unmanned Aerial Systems (UAS)* employé dans la version originale anglaise du présent Mémorandum se réfère aux véhicules aériens et à leurs éléments reliés qui sont manœuvrés sans pilote à bord. Les systèmes d'aéronefs sans pilote, ou « non habités », peuvent être pilotés à distance par un pilote humain, ou par un système de pilote automatique sans intervention humaine ; ils se présentent sous plusieurs formes, allant du véhicule aérien à voilure fixe (avion) à ceux à voilure tournante (hélicoptère) de type monorotor ou multirotor. Ces systèmes sont parfois désignés en anglais par l'expression « *Unmanned Aircraft Systems* ». Aux fins du présent Mémorandum, aucune différence n'est établie entre ces deux expressions, qui sont toutes deux traduites ici par « systèmes d'aéronefs non habités ».

[2] Les cibles publiques, ou cibles civiles, telles que les définit le *Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte contre le terrorisme* sont des lieux qui participent à la vie de la communauté locale et à la prospérité économique, où la population se retrouve pour étudier, faire des courses, partager un repas, faire du commerce, se divertir, se recueillir ou voyager.

présent Mémorandum peut aider les pays à mettre en œuvre les obligations qui leur incombent en vertu de la RCSNU 1540.

À ce jour, l'utilisation de systèmes d'aéronefs non habités à des fins terroristes en dehors du cadre d'un conflit armé demeure relativement rare. Les terroristes ont privilégié d'autres types d'armes plus faciles à acquérir et à manœuvrer (par exemple les véhicules-bélier) ou plus meurtrières (par exemple l'utilisation au sol d'engins explosifs improvisés et d'armes à feu). Néanmoins, les systèmes d'aéronefs non habités ont fait l'objet d'importantes améliorations ces dernières années pour ce qui concerne la durée de vol, la facilité d'emploi, la possibilité d'être adaptés pour servir au lancement de charges sur des cibles, les capacités à se connecter à des réseaux civils de télécommunication et à d'autres systèmes d'aéronefs non habités ; l'ensemble de ces capacités technologiques est appelé à s'améliorer encore à un rythme accéléré. Les évolutions actuelles et celles que l'on peut anticiper pourraient venir à bout des contraintes qui ont jusqu'à présent limité l'utilisation de systèmes d'aéronefs non habités à des fins terroristes. À mesure que ces systèmes deviennent plus sophistiqués tout en étant plus faciles d'accès et moins onéreux, ils deviennent plus attractifs pour ceux qui veulent les utiliser à des fins terroristes. Leur disponibilité croissante dans le commerce reflète également la percée des systèmes d'aéronefs non habités de fabrication artisanale ou à usage récréatif. Grâce aux fonctions avancées d'autopilotage et à l'existence d'une communauté active de télépilotes amateurs sur Internet, la construction et la manœuvre de ces appareils sont devenues bon marché et accessibles à tous, même aux personnes peu qualifiées. Ainsi, les terroristes qui projettent d'adapter les systèmes en vente libre ou d'investir dans la fabrication artisanale de systèmes d'aéronefs non habités afin de contourner les restrictions gouvernementales ont une marge de manœuvre accrue. Parallèlement, les systèmes d'aéronefs non habités risquent de devenir de plus en plus difficiles à contrer au moyen des technologies *ad hoc* disponibles ou en cours de développement. À terme, les terroristes seront probablement en mesure d'utiliser des systèmes d'aéronefs non habités aux capacités technologiques équivalentes à celles des plateformes militaires actuelles.

Il convient d'observer que l'EIIL/*Da'esh* 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 Irak et en Syrie. Les connaissances et l'expérience ainsi acquises peuvent ensuite être rapportées depuis ces zones par les combattants terroristes étrangers[3] ou servir de modèles à des terroristes d'origine nationale, y compris ceux agissant seuls[4]. L'EIIL/*Da'esh* a incité dans sa propagande à utiliser des systèmes d'aéronefs non habités pour attaquer des cibles dans diverses régions de la planète. Au Moyen-Orient et en Afrique occidentale, d'autres groupes terroristes ont attaqué des cibles au moyen de systèmes d'aéronefs non habités transformés en armes.

Les bonnes pratiques non contraignantes contenues dans le *Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités* ont pour but d'informer les gouvernements et de leur donner des orientations en vue d'identifier, de concevoir et d'améliorer les politiques, les pratiques, les lignes directrices, les règlements, les programmes et les méthodes destinés à lutter contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités. 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 de ces sujets au cours de quatre ateliers régionaux tenus

[3] Pour des orientations concernant l'élaboration de réponses efficaces au phénomène des combattants terroristes étrangers, voir le *Mémorandum de La Haye-Marrakech sur les bonnes pratiques pour répondre plus efficacement au phénomène des combattants terroristes étrangers* du GCTF.

[4] Pour des orientations concernant le terrorisme d'origine nationale, voir les *Bonnes pratiques de Rabat–Washington en matière de prévention, de détection, d'intervention et de réponse au terrorisme d'origine nationale* du GCTF.

respectivement en Allemagne, en Jordanie, en République de Corée et aux Pays-Bas en 2018 et 2019. Il tire également des enseignements importants du *Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte contre le terrorisme*[5].

Le *Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités* identifie 26 bonnes pratiques regroupées en quatre domaines qu'il soumet à la considération des États :

1. Évaluation du risque, évaluation des points de vulnérabilité et sensibilisation : Les États devraient intégrer dans leurs procédures systématiques d'évaluation du risque l'utilisation potentielle à des fins terroristes de systèmes d'aéronefs non habités, afin d'identifier en collaboration avec les parties prenantes compétentes les points de vulnérabilité et les failles des systèmes de protection. Les États devraient envisager l'ensemble des modalités potentielles d'utilisation par les terroristes de systèmes d'aéronefs non habités, anticiper les avancées technologiques et tout autre facteur susceptible d'avoir une incidence sur la menace, et répondre à chaque modalité inédite ou innovante du recours à ces systèmes par les terroristes.
2. Meilleur partage des informations, participation des acteurs concernés et sensibilisation du public : Le caractère multidimensionnel de l'utilisation de systèmes d'aéronefs non habités à des fins terroristes exige une méthode globale et concertée associant les États, les organisations intergouvernementales régionales et internationales ainsi que des acteurs non conventionnels. Les efforts déployés au niveau national pour lutter contre la menace d'une utilisation à des fins terroristes de systèmes d'aéronefs non habités devraient être complétés par des mesures appliquées à l'échelle régionale et internationale, suivant les cas. Les États devraient également associer le grand public dans la promotion d'une pédagogie sur l'utilisation responsable des systèmes d'aéronefs non habités et encourager les réponses appropriées aux utilisations suspectes de ces systèmes.
3. 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 d'empêcher et de minimiser les possibilités de prolifération et d'utilisation malveillante de systèmes d'aéronefs non habités par des terroristes ou d'autres acteurs malintentionnés, de faciliter les mesures efficaces de lutte contre ces systèmes et de permettre le bon déroulement et l'efficacité des enquêtes, poursuites et sanctions suite à des incidents impliquant des systèmes d'aéronefs non habités. Les gouvernements devraient également élaborer des stratégies de gestion et d'atténuation des crises afin d'apporter une réponse appropriée aux incidents impliquant des systèmes d'aéronefs non habités.
4. 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 ; cela suppose d'équiper et de former les autorités compétentes afin qu'elles puissent identifier et contrer les systèmes d'aéronefs non habités exploités dans l'intention de nuire. Avant de recourir à des contre-mesures, les États devraient évaluer et atténuer, en coopération avec les parties intéressées, les effets négatifs de ces contre-mesures, tout en gardant à l'esprit qu'elles mobilisent parfois des ressources considérables et entraînent des besoins importants en formation.

Les bonnes pratiques qui suivent portent sur le traitement de l'utilisation à des fins terroristes de systèmes d'aéronefs non habités en dehors du contexte des conflits armés. L'utilisation de systèmes d'aéronefs non habités par des acteurs violents non étatiques lors d'un conflit armé peut exiger que

[5] Le *Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte contre le terrorisme* a identifié l'acquisition de connaissance et la lutte contre les utilisations malveillantes des nouvelles technologies, dont les systèmes d'aéronefs non habités, comme un domaine d'attention prioritaire pour les gouvernements et le secteur privé.

les États prennent des mesures comparables aux bonnes pratiques contenues dans le présent Mémorandum ; toutefois, celles-ci n'ont pas pour but d'être appliquées dans un tel contexte ni en réponse à l'utilisation de systèmes d'aéronefs non habités par les forces de défense d'un pays engagé dans un conflit armé[6]. Si les bonnes pratiques contenues dans ce Mémorandum ont été spécifiquement rédigées dans le seul but de répondre à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, elles peuvent néanmoins se révéler utiles pour faire face à d'autres usages malveillants (notamment par des entreprises criminelles) ou négligents, irréfléchis ou imprudents dans un contexte national[7]. Ce Mémorandum ne prétend pas être exhaustif. Il est recommandé aux États de consulter d'autres documents et initiatives existants ou futurs, d'envergure régionale et internationale, afin de s'assurer d'avoir mis en place des mesures efficaces pour contrer les systèmes d'aéronefs non habités[8].

Lors de chacune des étapes de leurs efforts pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, les États doivent s'assurer qu'ils respectent les obligations qui leur incombent au titre du droit national et du droit international. En outre, les États ne doivent pas entraver les usages bénéfiques et légitimes des systèmes d'aéronefs non habités.

Bonnes pratiques

Évaluation du risque, évaluation des vulnérabilités et sensibilisation

Bonne pratique n° 1 : Inclure l'utilisation potentielle par des terroristes de systèmes d'aéronefs non habités dans les évaluations systématiques du risque.

Si les systèmes d'aéronefs non habités sont principalement utilisés à des fins légitimes et bénéfiques, et continueront de l'être, ils peuvent aussi faire l'objet d'une utilisation détournée par des terroristes. Les utilisations à des fins terroristes de systèmes d'aéronefs non habités en dehors du cadre d'un conflit armé ont été jusqu'à présent relativement rares. Néanmoins, en raison de la sophistication croissante des pratiques dont font preuve certains groupes terroristes ou certains terroristes agissant seuls, ainsi que du développement continu des systèmes d'aéronefs non habités disponibles et de leurs usages commerciaux, la probabilité d'une intensification des expérimentations et utilisations de ces systèmes à des fins terroristes s'accroît. L'évaluation du risque devrait s'appuyer sur les évolutions et enseignements passés pertinents et permettre aux États d'intégrer les informations existantes et les données du renseignement dans une approche de la menace fondée sur le risque. Les États devraient évaluer la probabilité que des systèmes d'aéronefs non habités soient utilisés à des fins terroristes, ainsi que les vulnérabilités par rapport à ce risque et ses conséquences potentielles, tout en comparant ce risque avec celui découlant d'autres menaces. Les États seront ainsi en mesure

[6] Par conséquent, sauf mention contraire, l'expression « utilisation à des fins terroristes de systèmes d'aéronefs non habités » et les formulations similaires se réfèrent exclusivement à l'utilisation par des terroristes de systèmes d'aéronefs non habités en dehors du contexte des conflits armés.

[7] Le présent Mémorandum traite des méthodes concrètes permettant de contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités en dehors du contexte des conflits armés ; l'expression employée dans ce document est « utilisation à des fins terroristes de systèmes d'aéronefs non habités » et d'autres similaires. La possibilité d'appliquer certaines bonnes pratiques à l'utilisation de ces systèmes d'aéronefs non habités par d'autres acteurs malveillants, ou par des utilisateurs négligents, irresponsables ou imprudents dépend de chaque situation particulière.

[8] Le Conseil de sécurité des Nations Unies a déjà reconnu la menace posée par les systèmes d'aéronefs non habités utilisés par des terroristes, par exemple dans la RCSNU 2370 (2017). INTERPOL a prévu la publication des Lignes directrices sur ce sujet (*Drone Response and Forensic Guidelines*) dans le courant de l'année 2019.
Concernant les initiatives de la Direction exécutive du Comité contre le terrorisme (DECT) du Conseil de sécurité des Nations Unies, voir les notes 15 et 16.

d'établir l'ordre de priorité de la menace liée à une utilisation à des fins terroristes de systèmes d'aéronefs non habités par rapport à d'autres menaces.

Certaines évolutions du terrorisme transnational qui n'ont, de prime abord, pas trait à une menace spécifique d'utilisation à des fins terroristes de systèmes d'aéronefs non habités peuvent néanmoins avoir une incidence sur cette menace. Par exemple, les combattants terroristes étrangers de retour dans leur pays semblent à première vue poser un ensemble de problèmes sans rapport avec celui de l'utilisation détournée à des fins terroristes de systèmes d'aéronefs non habités. Néanmoins, leur retour peut entraîner une menace accrue d'une telle utilisation dans leur pays d'origine, voire même dans des pays tiers, s'ils disposent des connaissances nécessaires pour fabriquer des systèmes d'aéronefs non habités, les utiliser et les transformer en armes. Compte tenu du caractère parfois transnational des activités terroristes, les États devraient améliorer leur coopération avec un partage des leçons tirées ainsi que des informations en matière de poursuites et des éléments de preuve sur l'utilisation avérée et projetée de systèmes d'aéronefs non habités, tout comme sur les transferts et la prolifération d'équipements, d'arsenaux et de compétences revêtant une importance significative[9].

Les États devraient se maintenir au fait des évolutions technologiques et commerciales aussi bien d'ordre général que spécifiquement liées aux systèmes d'aéronefs non habités, ainsi que des usages innovants et souvent légitimes qui sont faits et seront faits à l'avenir de ces systèmes (par exemple, pour l'épandage aérien des cultures, usage qui pourrait inspirer aux terroristes d'utiliser ces systèmes pour pulvériser des agents biologiques), et évaluer leur impact dans le contexte plus large des menaces. Les innovations technologiques (telles que le perfectionnement des systèmes d'aéronefs non habités en les dotant de l'intelligence artificielle, la reconnaissance automatique d'images, la propulsion par réaction, les réseaux 5G, les technologies d'évitement des collisions) pourraient modifier l'échelle, la portée, l'ordre de grandeur, la capacité létale et les trajectoires de la menace posée par leur utilisation à des fins terroristes. Les États devraient assurer un suivi permanent de ces évolutions et de leurs conséquences potentielles sur le risque posé par les systèmes d'aéronefs non habités. En outre, les États devraient procéder à la recherche et au suivi actifs et continus des dernières évolutions technologiques, des usages innovants potentiels et des capacités émergentes observées tant dans les systèmes d'aéronefs non habités en vente libre que dans ceux de fabrication artisanale. Les États pourraient aussi obtenir des éclaircissements sur ce sujet auprès d'experts et d'institutions de recherche ainsi qu'en menant des activités innovantes telles que des « hackathons », événements durant lesquels des groupes de développeurs (amateurs) spécialisés dans un domaine particulier se réunissent pour tester ou programmer de nouvelles configurations matérielles ou logicielles. Une connaissance des principes essentiels des technologies actuelles et à venir en matière de systèmes d'aéronefs non habités contribuera à préparer les États à l'élaboration de contre-mesures efficaces.

Une crainte souvent exprimée au sujet de l'évolution des technologies liées aux systèmes d'aéronefs non habités concerne les « essaims de drones », c'est-à-dire des systèmes d'aéronefs non habités opérant simultanément en grand nombre et capables de communiquer les uns avec les autres en formant une nuée massive et coordonnée d'appareils. Les « essaims de drones » représentent une menace importante pour diverses raisons, en particulier leur capacité à partager des informations en temps réel et leur aptitude à agir et à se coordonner les uns aux autres, obtenant ainsi une résilience qui parvient à saturer les efforts de défense. Cette menace est l'un des nombreux exemples qui justifient que les États intègrent en permanence les innovations technologiques dans l'évaluation systématique des menaces.

[9] Pour des orientations sur le partage des éléments de preuve en lien avec les poursuites pénales, voir les *Recommandations d'Abuja sur la collecte, l'utilisation et le partage d'éléments de preuve aux fins des poursuites pénales de terroristes présumés*.

Bonne pratique n° 2 : Reconnaître la multiplicité d'utilisations possibles par les terroristes de systèmes d'aéronefs non habités.

Les États devraient envisager toutes les utilisations possibles et innovantes par les terroristes de systèmes d'aéronefs non habités. Si les attentats terroristes perpétrés au moyen de ces systèmes ou avec l'appui de ces systèmes sont ceux qui ont le plus fort impact dans une perspective de sécurité nationale, les États devraient prendre conscience de la diversité des usages malveillants potentiels de ces systèmes. Les utilisations rapportées jusqu'à présent, principalement dans le contexte de conflits armés, vont des attentats physiques[10] (par exemple en chargeant un engin explosif improvisé à bord d'un système d'aéronef non habité dans le but de larguer des munitions ou d'effectuer une frappe directe [attentat-kamikaze] à l'appui d'une action principale ou pour cibler des agents de première ligne) à la collecte de données de renseignement et la conduite d'opérations de surveillance et de reconnaissance ; l'observation de cibles, protocoles de sécurité et structures de comportement ; le recours aux systèmes d'aéronefs non habités pour améliorer la précision des tirs indirects ; l'enregistrement de séquences vidéo à des fins de propagande terroriste ; la perturbation, l'intrusion malveillante et la paralysie d'infrastructures clés, du trafic aérien et d'actifs économiques; la contrebande de marchandises illicites, transfrontalière ou destinée à des zones sensibles. Les systèmes d'aéronefs non habités peuvent également être utilisés pour faire diversion et pour brouiller ou perturber l'action des forces de l'ordre, ou encore à des fins d'intimidation ou pour déclencher des mouvements de panique dans les rassemblements de foule.

Au même titre que ces modalités d'utilisation pléthoriques, les cibles de l'utilisation à des fins terroristes de systèmes d'aéronefs non habités sont extrêmement variées. Il peut s'agir de cibles gouvernementales, économiques et autres infrastructures critiques[11] ou bien de cibles civiles[12] ; peuvent être visées des personnalités en vue, des personnes choisies au hasard, ou encore la foule rassemblée lors de grands évènements publics (manifestations sportives, concerts, défilés, etc.). Les attentats impliquant des systèmes d'aéronefs non habités peuvent avoir pour but d'entraver le fonctionnement d'infrastructures critiques ou économiques. Enfin, les terroristes peuvent aussi tenter de pirater des systèmes d'aéronefs non habités ou d'en détourner l'usage bénéfique ou récréatif prévu par les gouvernements ou le secteur privé afin de créer des perturbations ou de semer le chaos, de contourner ou fourvoyer les systèmes de contre-mesures, ou de contribuer à une cyberattaque.

Compte tenu de la diversité des modalités d'utilisation et des cibles, les États devraient procéder à une évaluation globale de la menace et envisager, tester, analyser et mettre en œuvre une pluralité de mesures différentes pour contrer cette menace. Les États auront toujours à prioriser certains scénarios de menace par rapport à d'autres, mais il est impératif que la gamme extensive des *modi operandi* potentiels soit prise en considération dans l'évaluation globale de la menace.

---

[10] Tels que les reconnaît la *Convention internationale pour la répression des attentats terroristes à l'explosif* (New York, 15 décembre 1997).

[11] Comme cela est expliqué dans le *CTED Trends Report: Physical Protection of Critical Infrastructure against Terrorist Attacks*, en dépit de différences mineures de définition suivant les pays, l'expression « infrastructures critiques » désigne les actifs, les systèmes ou les organisations chargés d'assurer et de maintenir des fonctions vitales pour la société, et qui sont indispensables à cette fin. Sans s'y limiter, cela recouvre les systèmes de télécommunication tels que la radio et la télévision ; les technologies de l'information telles que les points d'échange Internet ; les services d'intervention d'urgence ; les installations et infrastructures du secteur de l'énergie et les installations industrielles telles que les centrales nucléaires et les usines chimiques ; les infrastructures financières ; les services publics tels que les établissements de santé ; les systèmes de transport ; et le réseau d'approvisionnement en eau.

[12] Pour une définition des cibles civiles, voir la note 2.

Bonne pratique n° 3 : Entreprendre une évaluation globale des vulnérabilités afin d'identifier les failles des dispositifs de sécurité et de protection.

Compte tenu de la capacité des systèmes d'aéronefs non habités à contourner les dispositifs classiques de protection (par exemple les clôtures), certains sites par ailleurs bien protégés comme les centrales nucléaires ou les locaux diplomatiques se révèlent vulnérables aux attaques par des systèmes d'aéronefs non habités. Afin d'identifier les points de vulnérabilité existants et les failles de sécurité, les États devraient s'appuyer sur leur évaluation générale de la menace telle que décrite dans la Bonne pratique n° 1 pour entreprendre une évaluation exhaustive des vulnérabilités. Celle-ci devrait passer en revue les mesures de protection physiques et les procédures de sécurité et évaluer leur efficacité potentielle contre des attaques par des systèmes d'aéronefs non habités, en prenant en compte les principales caractéristiques de la menace, dont la vitesse et l'altitude de vol ; le temps limité dont disposent les forces de sécurité pour réagir ; et le fait que les acteurs malveillants peuvent manœuvrer à distance les systèmes d'aéronefs non habités. L'évaluation des points de vulnérabilité devrait aussi localiser les emplacements susceptibles de servir de sites de lancement de systèmes d'aéronefs non habités à proximité de cibles éventuelles.

Jusqu'à présent, la plupart des utilisations (ou tentatives d'utilisation) de systèmes d'aéronefs non habités à des fins terroristes ou criminelles en dehors du contexte des conflits armés ont eu pour cibles des sites gouvernementaux. Par conséquent, une attention particulière devrait être accordée à ces sites ainsi qu'aux fonctionnaires de l'État. Toutefois, cela ne signifie pas que d'autres infrastructures critiques[13] ou des cibles civiles[14] telles que les manifestations publiques, les hôtels et les aéroports sont moins intéressantes aux yeux des terroristes. Le nombre limité d'attentats perpétrés au moyen de systèmes d'aéronefs non habités contre des cibles non gouvernementales semble devoir être imputé non pas tant à un changement de tactique qu'aux limites actuelles inhérentes à ces systèmes. Compte tenu des évolutions attendues dans le domaine des systèmes d'aéronefs non habités, le risque d'attaques contre des cibles non gouvernementales devrait s'accroître, ce qui devra être pris en compte lors de l'évaluation de la vulnérabilité des cibles civiles et des infrastructures critiques non gouvernementales. Les États devront donner la priorité à la protection de certaines cibles, en se basant sur l'évaluation du risque et des vulnérabilités qu'ils auront effectuée.

Bonne pratique n° 4 : Mettre en commun les évaluations du risque effectuées au niveau intersectoriel.

En raison de l'utilisation croissante de systèmes d'aéronefs non habités par les services publics ou les entreprises (par exemple pour des interventions d'urgence, l'agriculture, la sécurité publique, l'aviation, les télécommunications, les services de santé publique), les différentes parties intéressées seront exposées à des niveaux de risque et des types de vulnérabilités pouvant varier pour ce qui a trait aux perturbations, troubles ou attaques dont elles pourraient faire l'objet impliquant des systèmes d'aéronefs non habités.

Compte tenu de l'ubiquité croissante des systèmes d'aéronefs non habités utilisés par de nombreux secteurs, qui parfois se recoupent, il faut accorder une attention particulière à l'analyse, l'examen et la comparaison des menaces communes ou spécifiques rencontrées par ces différents secteurs, qu'ils

[13] Pour des orientations générales concernant la protection des infrastructures critiques contre des attaques terroristes, voir : CTED [DECT], *Trends Report: Physical Protection of Critical Infrastructure against Terrorist Attacks*, et CTED [DECT], INTERPOL, Bureau de lutte contre le terrorisme (UNOCT), *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*.

[14] Pour des orientations générales concernant la protection des cibles civiles contre des attentats terroristes, voir le *Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte contre le terrorisme* du GCTF.

soient gouvernementaux ou non. Cela permettra d'améliorer la compréhension collective des risques encourus par chaque sphère d'activités. Le partage d'informations avec les parties prenantes concernées tel que le décrit la Partie II est essentiel pour atteindre cet objectif.

Bonne pratique nº 5 : Éviter le phénomène de lassitude face aux systèmes d'aéronefs non habités.

Nombre 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. Les gouvernements devraient prendre des mesures pour se prémunir contre ce phénomène de « lassitude face aux systèmes d'aéronefs non habités ».

Afin d'éviter la lassitude face aux systèmes d'aéronefs non habités, les gouvernements devraient pratiquer (à tous les niveaux) la transparence en matière de risque (étayée par des évaluations du risque documentées), diffuser des mises à jour régulières destinées aux fonctionnaires et dialoguer avec le grand public afin de l'associer à cet enjeu, comme le décrit la Bonne pratique nº 15. La création de méthodes permettant la notification de toute activité constatée ou suspecte de systèmes d'aéronefs non habités peut faire partie de cette approche afin d'aider les gouvernements et les organisations à constituer un socle de connaissances et de clairvoyance qui permettra par la suite d'effectuer des mises à jour et des évaluations du risque bien documentées. Cette approche, qui peut sembler contre-intuitive, est en réalité fondamentale. Une interaction constante et le partage d'informations sont les antidotes à la complaisance. Les gouvernements devraient maintenir ouvertes certaines voies de communication au sein du dispositif de protection du secret de la sécurité nationale afin d'informer les responsables et, si nécessaire, le public, des menaces liées à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités et des réponses à ces menaces.

Bonne pratique nº 6 : Sensibiliser davantage le public à la réalité de la menace sans pour autant alarmer inutilement la population.

Les États devraient prendre conscience de la nécessité urgente d'instaurer une meilleure sensibilisation et compréhension commune parmi les responsables politiques et le public concernant la menace de l'utilisation à des fins terroristes de systèmes d'aéronefs non habités ainsi que les dangers pour la sécurité découlant d'une utilisation négligente de ces appareils, sans pour autant alarmer inutilement la population du pays et sans mettre en péril les usages bénéfiques et légitimes des systèmes d'aéronefs non habités. La réussite de ces deux objectifs exige un subtil équilibrage. Les efforts de sensibilisation ne devraient pas banaliser la menace, mais il est tout aussi important de ne pas alarmer inutilement le public à l'égard des systèmes d'aéronefs non habités, qui continuent à faire l'objet de nombreuses utilisations pacifiques et productives. Les États devraient donc s'engager dans un dialogue constructif avec le public afin d'établir clairement en quoi consiste la menace que peuvent poser les utilisations illicites de systèmes d'aéronefs non habités, tout en faisant observer les bénéfices de ces systèmes dans leur utilisation courante. Les messages délivrés devraient souligner les obligations et responsabilités réglementaires. Des messages complémentaires pourraient mentionner dans des termes généraux et non classifiés les diverses contre-mesures adoptées pour assurer la sécurité du public, tout en apportant des conseils pratiques sur les réponses appropriées en cas d'incident impliquant des systèmes d'aéronefs non habités. La transparence des données, des statistiques et des chiffres relatifs à l'utilisation de systèmes d'aéronefs non habités est essentielle pour que les citoyens aient confiance dans les autorités chargées de la sécurité publique.

Diverses questions devraient être traitées, en particulier celles qui ont trait à la vie privée, à la réglementation régissant les responsabilités liées à la possession et à l'exploitation de systèmes d'aéronefs non habités dans le cadre de la gestion du trafic intra et transfrontalier de ces systèmes. La transparence des données, des statistiques et des chiffres liés à l'utilisation des systèmes d'aéronefs non habités par des terroristes ou à la menace de cette utilisation est essentielle à l'instauration et au maintien de la confiance des citoyens. Les activités à destination du grand public sont examinées et décrites en détail dans la Bonne pratique n° 15.

II. Meilleur partage des informations, participation des acteurs concernés et sensibilisation du public

Bonne pratique n° 7 : Définir et mettre en place l'échange de connaissances et le partage d'informations avec les acteurs concernés.

La menace terroriste liée aux systèmes d'aéronefs non habités a un caractère multidimensionnel et se propage au-delà des frontières. Par conséquent, elle exige une réponse intégrant une vaste coalition d'acteurs. Comme le soulignent les Bonnes pratiques n°s 9 à 15, les États devraient identifier les acteurs compétents avec lesquels il conviendra de procéder à un échange de connaissances et, s'il y a lieu, à un partage d'informations et de données du renseignement. Le partage d'informations devrait intervenir à chaque étape de la mise en œuvre des stratégies visant à contrer les systèmes d'aéronefs non habités. Les informations partagées devraient notamment porter sur les aspects suivants : la menace, au sens où la décrit la Bonne pratique n° 4 ; les règlements applicables sous différentes juridictions, afin de prévenir toute faille exploitable (par exemple, les différences dans les obligations incombant aux fabricants d'équiper leurs systèmes d'aéronefs non habités de solutions technologiques préventives) et de partager les pratiques optimales ; les auteurs d'incidents en lien avec le terrorisme impliquant des systèmes d'aéronefs non habités, et les poursuites pénales ; les réponses mises en place par les services chargés de l'application de la loi et d'autres acteurs ; l'efficacité respective de diverses contre-mesures dans différentes configurations opérationnelles.

Le partage d'informations exige que les États mettent en place un dialogue actif avec des acteurs clés. Lorsque cela n'a pas encore été fait, les États devraient veiller à désigner des points de contact qui auraient pour compétence de recevoir les informations pertinentes.

Bonne pratique n° 8 : Convenir d'une terminologie commune et d'outils permettant le partage d'informations.

Les parties prenantes doivent pouvoir se comprendre afin de partager efficacement leurs informations. L'emploi d'une terminologie et de définitions disparates peut saper la compréhension mutuelle. En vue d'une coopération efficace, les États et les organisations régionales et internationales devraient convenir d'une terminologie commune et de définitions normalisées pour communiquer sur les systèmes d'aéronefs non habités. Ce lexique commun peut être élaboré dans le cadre d'échanges intergouvernementaux comme le décrit la Bonne pratique n° 9, ou par des organisations régionales et internationales ou en collaboration avec elles comme le décrit la Bonne pratique n° 12. Plusieurs États et organisations régionales et internationales telles que l'Union européenne (UE) et l'Organisation du Traité de l'Atlantique Nord (OTAN) ont déjà lancé des initiatives visant à élaborer des lexiques communs. Les États devraient prendre en compte les efforts existants et envisager d'y participer et de les soutenir.

Un lexique commun devrait proposer, au minimum, une classification des différentes catégories de systèmes d'aéronefs non habités (par exemple, en fonction de leur taille ou de leurs capacités) et des

incidents qu'ils peuvent occasionner (par exemple, les incidents dus à la négligence ou les utilisations détournées à des fins terroristes). Bien que souhaitable, l'harmonisation totale de l'ensemble des définitions et classifications n'est pas indispensable, dans la mesure où il peut y avoir des différences mineures d'interprétation ou de pratiques d'un État à l'autre. Néanmoins, les États devraient mettre en commun tout ce qui leur est indispensable pour effectuer une évaluation conjointe du risque et des vulnérabilités et pour collaborer à l'élaboration et à la mise en œuvre de leurs règlements, politiques et contre-mesures respectives. Si un lexique commun est élaboré, les États devraient, dans la mesure du possible, employer ces définitions concertées dans les textes de la législation nationale applicables aux systèmes d'aéronefs non habités. Cela facilitera l'échange de connaissances, la coopération intergouvernementale et l'examen comparatif du succès enregistré par les divers règlements, politiques et contre-mesures.

Lors de l'élaboration d'un lexique commun, les États devraient également s'efforcer d'élaborer des normes communes pour tester les systèmes d'aéronefs non habités et les contre-mesures prises à leur encontre. Il est essentiel que les États suivent les mêmes normes et protocoles lors de la comparaison des résultats obtenus par les contre-mesures.

De même, les États devraient veiller à recourir à un langage commun dans la collaboration avec des acteurs non étatiques (par exemple le secteur privé ou universitaire). Suivant la fréquence de cette coopération, les efforts d'harmonisation peuvent être effectués au cas par cas ou de manière permanente.

Le partage d'informations sur les incidents, les évolutions et les contre-mesures en lien avec l'utilisation à des fins terroristes de systèmes d'aéronefs non habités doit se faire en élaborant une base de données commune. Celle-ci devrait être gérée à l'échelle internationale, régionale, nationale ou infra-étatique (par exemple par le secteur universitaire ou privé) ; les États pourraient ainsi évaluer de manière réaliste la menace liée aux utilisations en lien avec le terrorisme de systèmes d'aéronefs non habités, les contre-mesures envisagées et toute information pertinente. Par conséquent, les États devraient procéder à la création commune de cette base de données ou bien, pour éviter la fragmentation des efforts, rejoindre les initiatives déjà crées par d'autres acteurs, en particulier INTERPOL. Toutefois, la collecte et l'archivage de ces données doivent faire l'objet de la plus grande vigilance afin qu'aucun point de vulnérabilité ni aucune information sensible en lien avec la sécurité ne puissent être divulgués.

Bonne pratique n^{o} 9 : Renforcer l'échange de connaissances et le partage d'informations au niveau intergouvernemental.

Afin de lutter contre la menace transnationale posée par l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, les États devraient s'efforcer de gagner en efficacité en partageant avec d'autres pays et gouvernements leurs meilleures pratiques ainsi que les enseignements qu'ils ont tirés de l'expérience. Il est essentiel de réunir régulièrement les principaux acteurs nationaux et, le cas échéant, les acteurs régionaux et internationaux afin d'examiner, entre autres, l'évolution technologique des systèmes d'aéronefs non habités, les meilleures méthodes pour contrer la menace posée par leur utilisation à des fins terroristes et les lacunes potentielles des pratiques et des politiques en la matière, tant à l'échelle d'un pays qu'au niveau international. Pour faciliter la coopération internationale en la matière, il conviendrait d'instituer ou d'améliorer l'échange de connaissances au niveau intergouvernemental. Il serait également bénéfique de tirer parti des centres de coordination régionaux qui facilitent le partage d'informations pertinentes au niveau régional. Lorsqu'ils existent, les centres régionaux de lutte contre le terrorisme peuvent servir de plateformes pour ces échanges. En l'absence de tels centres, les États pourraient envisager leur création afin de

partager des informations générales sur les activités terroristes dans la région et plus particulièrement sur la menace d'utilisation à des fins terroristes de systèmes d'aéronefs non habités.

Les échanges de connaissances au niveau international permettent également de comparer les différentes méthodes gouvernementales ainsi que l'incidence des contraintes constitutionnelles ou légales sur les règlements, incidence qui peut varier d'un pays à l'autre. La prise de conscience de ces aspects est importante pour comprendre et combattre les stratégies déployées par les terroristes afin de tirer avantage des disparités entre les règlements, les autorités compétentes et les politiques sous différentes juridictions. Les informations partagées peuvent également porter sur les enseignements tirés lors des poursuites pénales et des activités de détection et de répression.

Les informations relatives aux activités terroristes sont souvent classifiées et ne peuvent donc pas être partagées facilement avec d'autres gouvernements. Par conséquent, les États doivent s'efforcer de définir quelles sont les informations clés ou les éléments de renseignement qui peuvent être déclassifiés, dans la mesure du possible, afin d'assurer un partage d'informations efficace.

Bonne pratique n° 10 : Mettre en place et améliorer la coordination entre les autorités nationales et locales.

Si l'élaboration des stratégies visant à contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités est le plus souvent du ressort des niveaux national, régional ou international, ce sont très probablement les autorités locales qui seront chargées d'appliquer concrètement ces stratégies et de contrer les systèmes d'aéronefs non habités. Il est donc impératif d'assurer le partage d'informations (et de renseignement) en renforçant la coordination entre les autorités nationales et locales du pays et d'améliorer la perception de la menace au niveau local.

Une telle coordination réclame des mesures variées. Les autorités locales devraient être formées pour apprendre à distinguer les utilisations légitimes de systèmes d'aéronefs non habités de celles qui ont une visée terroriste ; savoir répondre à une activité suspecte ; savoir utiliser les contre-mesures ; et, le cas échéant, faire appel aux capacités nationales de soutien, lorsque celles-ci existent. De même, les autorités locales devraient être encouragées à partager activement avec le niveau national leurs expériences, leurs meilleures pratiques et les leçons apprises. Un dispositif normalisé de notification des incidents liés aux systèmes d'aéronefs non habités peut également améliorer la coordination entres les niveaux local et national.

Afin de garantir l'efficacité de la coordination entre les autorités nationales et locales, les États devraient désigner un point de coordination national dans le domaine de la lutte contre les systèmes d'aéronefs non habités, ainsi que les points focaux correspondants au niveau local. Le point de coordination national peut être chargé d'élaborer et de diffuser un plan d'action national auprès des points focaux locaux, qui résumerait les différentes politiques, procédures, contre-mesures et stratégies en la matière. Autre possibilité, les autorités locales pourraient être chargées d'élaborer des plans d'action locaux qui seront par la suite examinés par l'autorité nationale de coordination, qui en assurera l'exécution coordonnée.

Lorsque les compétences visant à contre les systèmes d'aéronefs non habités se répartissent entre des autorités nationales et locales distinctes, les États devraient régulièrement organiser des exercices communs destinés à toutes les unités concernées.

Bonne pratique nº 11 : Mettre en place et améliorer la coordination avec les forces nationales de défense.

Si les bonnes pratiques contenues dans ce Mémorandum se limitent à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités en dehors du contexte des conflits armés, les États devraient néanmoins prendre en considération l'expérience acquise et les enseignements tirés par les forces nationales de défense. 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.

Afin de se prémunir contre les utilisations malveillantes et dangereuses de systèmes d'aéronefs non habités, les États devraient chercher activement à se former auprès des forces de défense au niveau national, régional et international. Ce faisant, les États devraient prendre en considération les caractéristiques particulières de l'action militaire. Il est important d'observer 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.

Bonne pratique nº 12 : Mettre en place et améliorer la coordination avec les organisations régionales et internationales.

Les États devraient également encourager et pratiquer le partage d'informations avec les organisations gouvernementales régionales et internationales. Ces organisations constituent une plateforme reconnue pour accueillir et soutenir la coopération interétatique, diffuser des connaissances clé et analyser les ressources dont disposent les États (par exemple concernant l'incidence de l'évolution technologique des systèmes d'aéronefs non habités sur la lutte contre le terrorisme). Les États devraient donc veiller à recenser les organisations régionales et internationales compétentes.

Par exemple, la Direction exécutive du Comité contre le terrorisme (DECT) du Conseil de sécurité des Nations Unies a mis en place diverses initiatives qui pourraient être utiles pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités et pour d'autres questions connexes[15]. La DECT est donc un acteur clé de l'évaluation des failles de la protection contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités et de l'élaboration de stratégies de lutte. Elle constitue en outre une plateforme intéressante pour le partage de bonnes pratiques et de mesures réussies de lutte contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, en plus de servir de catalyseur pour la coopération et les partenariats avec d'autres acteurs compétents (en particulier le secteur universitaire[16], le secteur privé et d'autres organisations régionales et internationales).

---

[15] Au cours de cette initiative, la DECT a consacré une livraison du *CTED Trends Alert* aux risques posés par l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, dans le but de sensibiliser les Nations Unies, les États et d'autres acteurs pertinents à cette menace. Le *Trends Alert* présente également un recueil systématique des différentes approches, problématiques et initiatives nationales, régionales et internationales. Concernant les efforts de la DECT en matière de protection des infrastructures critiques contre les attaques terroristes, voir la note 11. Pour des orientations complémentaires destinées aux États, y compris en matière de prévention de la prolifération d'armements aux mains des terroristes, voir : CTED (DECT), *Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions.* Concernant la question de la circulation des combattants terroristes étrangers, voir : CTED (DECT), *Madrid Guiding Principles* [Principes directeurs de Madrid relatifs aux combattants terroristes étrangers].

[16] La DECT a lancé son Réseau global de recherche (*Global Research Network [GRN]*) en 2015. Il vise à tirer parti de l'expérience que les instituts de recherche et les groupes d'experts du monde entier ont accumulée sur les sujets en lien avec le terrorisme.

Bonne pratique n° 13 : Mettre en place et améliorer la coordination avec les autorités compétentes de l'aviation civile, les prestataires de services de navigation aérienne et les organismes régissant la sécurité et les communications dans le domaine de l'aviation.

Les autorités compétentes de l'aviation, les prestataires de services de navigation aérienne et les agences nationales, régionales et internationales compétentes en matière de gouvernance de la sécurité et des communications dans le domaine de l'aviation sont des acteurs importants de la lutte contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, et certains ont déjà déployé des efforts importants en la matière[17]. Les États devraient mettre en place des partenariats avec ces autorités, ces prestataires et ces agences, à deux égards en particulier.

La participation des autorités compétentes de l'aviation, des prestataires de services de navigation aérienne et des organismes régissant la sécurité et les communications de l'aviation est indispensable lors de la conception des règlements régissant la sécurité de l'exploitation des systèmes d'aéronefs non habités et le trafic aérien ainsi que pour assurer la future gestion du trafic. Dans la plupart des pays, les autorités compétentes de l'aviation sont responsables de la réglementation de la sécurité aérienne, tandis que le contrôle aérien relève soit de ces autorités compétentes, soit des prestataires de services de navigation aérienne ; par conséquent, ces entités sont probablement en mesure de détecter en vol les systèmes non conformes d'aéronefs non habités. Au moment d'adopter des règlements et de mettre en place des mesures visant à réguler les vols d'aéronefs non habités, les États devraient collaborer avec les autorités compétentes de l'aviation, les prestataires de services de navigation aérienne et les organismes régissant la sécurité et les communications de l'aviation et tirer les enseignements de leur expérience. Les États devraient également être en contact permanent avec ces entités afin de s'assurer que les informations sur les systèmes d'aéronefs non habités suspects sont communiquées en temps réel.

Les autorités compétentes de l'aviation, les prestataires de services de navigation aérienne et les organismes régissant la sécurité et les communications de l'aviation sont également des acteurs essentiels lors du lancement de contre-mesures visant des systèmes d'aéronefs non habités. Compte 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 États devraient coordonner avec les agences gouvernementales pertinentes leurs activités de lutte contre les systèmes d'aéronefs non habités afin que ces agences puissent les aider à atténuer autant que possible les conséquences indésirables des contre-mesures. Les États devraient également coopérer avec ces entités lors de la conception et de l'évaluation des contre-mesures, 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.

[17] L'OACI a rendu publique sa *Trousse d'outils de l'OACI pour les UAS* qui décrit les meilleures pratiques et fournit des recommandations pour réglementer l'exploitation des systèmes d'aéronefs non habités et pour mettre en place des programmes de formation et de sensibilisation, ainsi qu'un aperçu des règlements étatiques actuels en la matière dans différents pays, une campagne de sensibilisation et du matériel didactique destiné aux pilotes amateurs. L'Association internationale du transport aérien (IATA) a publié un Bulletin d'information sur les considérations à prendre en compte en matière de protection des appareils de l'aviation contre les systèmes d'aéronefs non habités : *IATA Information Bulletin*: *Key Considerations when protecting manned aviation from drones*. La Federal Aviation Administration (FAA) des États-Unis a créé une bibliothèque très complète de ressources d'orientation pour les pilotes de systèmes d'aéronefs non habités, les autorités et les gouvernements, y compris une application mobile pour pilotes amateurs.

Bonne pratique n° 14 : Mettre en place et améliorer la coordination avec le secteur privé et d'autres acteurs non conventionnels.

La coopération avec le secteur privé et avec d'autres acteurs non conventionnels est également indispensable pour contrer l'utilisation détournée à des fins terroristes de systèmes d'aéronefs non habités. Ces acteurs partagent avec les États de nombreux intérêts en faveur de la lutte contre l'utilisation par des terroristes de systèmes d'aéronefs non habités. Les partenariats public-privé ont fait preuve d'une certaine efficacité dans d'autres domaines de la lutte contre le terrorisme, en particulier la lutte contre le financement du terrorisme et la protection des cibles civiles. Les partenariats public-privé peuvent recouvrir un ou plusieurs secteurs d'activité et parties prenantes et devraient être considérés comme une composante essentielle des stratégies réussies de lutte contre les systèmes d'aéronefs non habités.

La participation active de représentants du secteur privé lors d'ateliers régionaux a démontré la préoccupation du secteur privé concernant l'utilisation à des fins terroristes de systèmes d'aéronefs non habités et sa volonté de partager son expertise spécifique afin de contribuer à une stratégie globale de lutte contre ce type d'utilisation de systèmes d'aéronefs non habités.

Les fabricants de systèmes d'aéronefs non habités peuvent doter leurs appareils de modalités de détection précoce (par exemple grâce aux fonctionnalités de détection à distance) et d'outils de prévention (par exemple grâce aux fonctionnalités de géo-détection et aux barrières géo-localisées activées à l'approche d'une zone sensible) afin de contrer les utilisations malveillantes de ces systèmes. Les concepteurs de dispositifs de lutte contre les systèmes d'aéronefs non habités peuvent apporter de nouveaux éclairages sur les contre-mesures. D'autres secteurs peuvent également apporter une contribution intéressante, par exemple le secteur des télécommunications pour la fourniture de données en temps réel sur les vols au-dessus de certaines zones déterminées. En outre, au lendemain d'un incident le secteur privé pourrait être apte et disposé à partager des informations sur les opérateurs de systèmes d'aéronefs non habités suspectés d'avoir pris part à des actions répréhensibles, ou à communiquer d'autres données criminalistiques utiles (par exemples des données géo-localisées).

Comme le détaille la Bonne pratique n° 17, les vendeurs de systèmes d'aéronefs non habités peuvent jouer un rôle actif pour prévenir la prolifération illicite de ces systèmes et de leurs équipements reliés. Les États devraient s'efforcer de sensibiliser les vendeurs de systèmes d'aéronefs non habités afin qu'ils détectent et notifient les acquisitions suspectes.

Les États pourraient instaurer un dialogue permanent avec le secteur privé et, sans porter préjudice à ses intérêts économiques légitimes, définir et rendre obligatoires la notification d'informations et l'application de certaines mesures destinées à améliorer la sécurité, dans la mesure où ces exigences peuvent raisonnablement être imposées au secteur privé. Il pourrait s'agir des aspects suivants : informations sur les évolutions technologiques attendues ; intégration d'outils de détection précoce ou d'outils préventifs (par exemple, dispositifs de détection à distance et barrières géo-localisées) tels que décrits ci-dessus et de solutions technologiques à l'appui des contre-mesures statiques (par exemple, récepteurs paramétrés spécifiquement pour les fréquences utilisées par les services de détection et de répression) ; dispositifs robustes intégrés aux systèmes d'aéronefs non habités afin de prévenir leur piratage illicite, mises à jour périodiques de sécurité incluses ; fourniture des données de vol (en temps réel), éventuellement rendues anonymes ; systèmes d'aide à l'enregistrement (par exemple, dispositifs bloquant le moteur tant que l'enregistrement du système d'aéronef non habité n'a pas été validé) ; information du public sur la réglementation applicable et les mesures préventives (au moyen de brochures ou d'informations en ligne) et formations destinées aux pilotes.

Les États devraient également collaborer avec les organisateurs de manifestions publiques de grande envergure et prendre acte de leur expérience. Ces manifestations sont généralement précédées d'une évaluation complète de la sécurité et d'une planification du dispositif de sécurité qui peuvent se révéler utiles lors de l'élaboration d'une stratégie plus large visant à contrer les systèmes d'aéronefs non habités.

Enfin, les universités devraient jouer un rôle dans la lutte contre la menace d'une utilisation à des fins terroristes de systèmes d'aéronefs non habités. Le milieu universitaire est un acteur essentiel de l'évaluation de la menace terroriste et des principales évolutions en lien avec le terrorisme, et joue également un rôle dans la recherche sur les avancées technologiques des systèmes d'aéronefs non habités et sur les contre-mesures applicables.

Bonne pratique n° 15 : Dialoguer avec le grand public et l'associer aux usages sûrs des systèmes d'aéronefs non habités et aux réponses appropriées en cas d'utilisation de ces systèmes à des fins terroristes.

Les systèmes d'aéronefs non habités devenant de plus en plus accessibles aux pilotes amateurs et aux entreprises privées, le nombre de ces systèmes opérant à des fins récréatives ou commerciales est appelé à augmenter significativement. Si les États devraient s'abstenir d'interdire et de restreindre ces usages légitimes et bénéfiques, il est néanmoins vital de s'assurer que le public connaît et respecte la réglementation et les politiques applicables aux systèmes d'aéronefs non habités, comme le décrit en détail la Bonne pratique n° 17. À terme, cela permettra tant au public qu'aux autorités compétentes de différencier les usages légitimes des utilisations à des fins terroristes, et réduira le risque de fausses alertes et de lassitude face aux systèmes d'aéronefs non habités.

Par conséquent, les États devraient dialoguer avec le public afin de le sensibiliser à la sécurité et à la conformité des utilisations de systèmes d'aéronefs non habités. La sécurité dont il s'agit doit recouvrir l'ensemble des contraintes d'exploitation exigées des opérateurs de systèmes d'aéronefs non habités, comme le décrit la Bonne pratique n° 17. La communication préventive permet de faire connaître et de rendre accessibles au public les règles et règlements applicables dans le pays ainsi que les mesures et politiques relevant du principe de précaution. Cela peut être fait au moyen d'informations en ligne, de brochures explicatives fournies par les fabricants avec leur produit, et de formations obligatoires ou volontaires à l'intention des télépilotes. Les États devraient également veiller à diffuser des informations et à mettre en place une signalétique claire afin que le public connaisse les zones d'exclusion aérienne et, dans la mesure du possible, faire en sorte que le tracé de ces zones soit intégré dans les logiciels des systèmes d'aéronefs non habités, comme le décrit la Bonne pratique n° 14.

Enfin, les États devraient expliquer au grand public comment réagir en cas d'utilisation à des fins terroristes de systèmes d'aéronefs non habités. Premièrement, le public pourrait être associé à la détection des systèmes d'aéronefs non habités suspects. Outre la sensibilisation générale à la menace, telle que décrite dans la Bonne pratique n° 6, les États devraient définir et (dès lors qu'il en va de la sécurité nationale) expliquer au public quels sont les signes éventuellement révélateurs d'une activité non autorisée de systèmes d'aéronefs non habités, en précisant à qui et comment notifier l'observation d'une telle activité. Deuxièmement, le public devrait être formé aux réponses appropriées en cas d'incidents impliquant des systèmes d'aéronefs non habités. Ceci devrait être fait de manière à ne pas alarmer inutilement le public, comme le conseille la Bonne pratique n° 6, et en veillant à éviter de provoquer une lassitude face aux systèmes d'aéronefs non habités, comme le souligne la Bonne pratique n° 5.

III. Mise en œuvre de politiques et de règlements, planification de la gestion des crises

Bonne pratique n° 16 : Se conformer aux obligations nationales et internationales et respecter les utilisations bénéfiques des systèmes d'aéronefs non habités ainsi que les intérêts économiques légitimes.

Les États doivent s'assurer qu'ils ont pris toutes les mesures nécessaires pour respecter les obligations qui leur incombent au titre du droit national et du droit international. De même, les États ne devraient pas entraver sans motif les utilisations bénéfiques des systèmes d'aéronefs non habités ni porter atteinte aux intérêts économiques légitimes du secteur des systèmes d'aéronefs non habités.

Bonne pratique n° 17 : Concevoir et mettre en œuvre des règlements et des politiques minimisant le risque d'utilisation détournée de systèmes d'aéronefs non habités par des terroristes.

Les États ne devraient pas se limiter aux seuls règlements et politiques destinés à atténuer l'impact de l'utilisation à des fins terroristes de systèmes d'aéronefs non habités. L'objet des règlements et des politiques mis en œuvre par les États devrait plutôt être de minimiser le risque d'utilisation détournée de ces systèmes, quel qu'en soit l'auteur. Ce faisant, les États devraient s'assurer qu'ils n'entravent pas sans motif valable les utilisations bénéfiques de systèmes d'aéronefs non habités. Le cadre réglementaire et les politiques visant à minimiser le risque d'utilisation détournée de systèmes d'aéronefs non habités devraient reposer sur trois composantes.

Premièrement, les États devraient adopter des règlements et des politiques visant à assurer la visibilité au sein de l'espace aérien. Pour ce faire, la méthode la plus efficace consiste à imposer des mesures d'identification électronique à distance et de détection précoce permettant de contrôler tous les systèmes d'aéronefs non habités présents dans un espace aérien déterminé, comme le décrit la Bonne pratique n° 18.

Deuxièmement, les États devraient adopter des règlements et des politiques imposant des restrictions appropriées à l'exploitation des systèmes d'aéronefs non habités, y compris la restriction de leur prolifération illégale. Il peut s'agir, en particulier, de règlements permettant aux États de surveiller et de suivre les achats suspects de systèmes d'aéronefs non habités, par exemple à travers le contrôle des importations et exportations de ces systèmes et de leurs équipements reliés, ou de restrictions à l'achat de systèmes d'aéronefs non habités au-delà d'une certaine taille ou capacité. Afin d'empêcher le contournement des règlements et des politiques de non-prolifération qui est souvent observé au niveau transfrontalier, les États devraient renforcer la coordination transnationale, notamment en consolidant les mécanismes de contrôle des exportations, par exemple par le biais d'organisations régionales et internationales afin d'échanger des informations critiques et d'appliquer les règles contre la prolifération transnationale illicite des technologies se rapportant aux systèmes d'aéronefs non habités[18].

Les règlements et les politiques relatifs aux restrictions exigées en matière d'exploitation des systèmes d'aéronefs non habités devraient couvrir l'octroi des licences aux opérateurs et les critères d'enregistrement des systèmes d'aéronefs non habités, comme le décrit la Bonne pratique n° 23. Le premier aspect pourrait inclure la formation obligatoire ou volontaire des opérateurs ainsi qu'un examen préalable à l'obtention de l'autorisation de manœuvrer un système d'aéronef non habité, et permettre également de procéder à une vérification des antécédents des télépilotes. En cas d'incident impliquant un système d'aéronef non habité, les dispositions sur les licences et l'enregistrement pourraient donner aux États la possibilité d'identifier l'opérateur et de faciliter l'enquête sur l'incident.

[18] Pour des orientations sur la gestion des frontières dans le contexte de la lutte contre le terrorisme, voir GCTF, *Bonnes pratiques dans les domaines de la sécurité et de la gestion des frontières dans un contexte de lutte contre le terrorisme visant à endiguer la circulation des combattants terroristes étrangers.*

Afin d'imposer des restrictions appropriées à l'exploitation de systèmes d'aéronefs non habités, les États devraient également envisager de fixer des limites raisonnables aux performances et capacités acceptables pour ces systèmes, dans le but de réduire les possibilités d'un usage détourné. Parmi d'autres mesures, les États devraient envisager d'imposer des limites à la vitesse et à l'altitude de vol dans certaines classes d'espace aérien, ainsi que des restrictions appropriées aux motifs autorisés de survol de systèmes d'aéronefs non habités dans certains espaces aériens, par exemple au-dessus d'infrastructures étatiques critiques ou de sites de sécurité nationaux. Les règlements de ce type permettent d'élaborer des normes comportementales qui peuvent donner aux personnels chargés de la sécurité des orientations pour repérer plus facilement les opérations non conformes qui peuvent exiger de recourir à des contre-mesures techniques ou à une action coercitive. Néanmoins, ces restrictions ne devraient pas imposer de contraintes excessives aux utilisations légitimes de systèmes d'aéronefs non habités.

Troisièmement, les États devraient aussi adopter des restrictions relatives au survol des personnes, des secours d'urgence et des opérations menées par les services de sécurité nationale et d'application de la loi, ainsi que d'infrastructures telles que les aéroports, des réunions de foule, des stades, etc. Ces restrictions pourraient être appliquées en faisant appel à des dispositifs de géo-détection et de balisage géolocalisé comme le décrit la Bonne pratique n° 23, ou, dans certaines situations exceptionnelles, en recourant à des contre-mesures cinétiques ou non cinétiques, comme le décrit la Bonne pratique n° 24.

Bonne pratique n° 18 : Concevoir et mettre en œuvre des règlements et des politiques permettant la détection de systèmes d'aéronefs non habités, ainsi que des contre-mesures efficaces.

De nombreux pays n'ont pas adopté de règlements ni de politiques leur permettant d'assurer une détection efficace des systèmes d'aéronefs non habités ni d'apporter une réponse effective aux utilisations détournées de ces systèmes, notamment à travers des mesures coercitives ou réglementaires à l'encontre des opérateurs. Si la plupart des gouvernements reconnaissent la nécessité de ces règlements et politiques, le processus est rendu difficile par la complexité du sujet, ses particularités techniques et la participation et responsabilités communes de plusieurs agences et organismes nationaux, internationaux et régionaux. Néanmoins, pour éviter une situation de flou juridique et permettre à l'ensemble des acteurs compétents, dont les services chargés de l'application de la loi, de contrer efficacement les menaces en lien avec le terrorisme posées par les systèmes d'aéronefs non habités, il est indispensable que les règlements et les politiques soient déjà en vigueur avant la survenue d'un incident. Ces règlements et politiques sont particulièrement nécessaires s'agissant des restrictions imposées à l'exploitation des systèmes d'aéronefs non habités, comme le décrit la Bonne pratique n° 17.

Les États devraient déterminer avec soin quels sont les acteurs prioritaires qu'il convient de doter de capacités de détection et de lutte contre les systèmes suspects d'aéronefs non habités, et vérifier que les acteurs identifiés possèdent les compétences techniques et le savoir-faire pour exercer ces capacités sans compromettre la sécurité et l'efficacité du système aérien, les réseaux de communication ou le droit à la vie privée. Il est vital de recourir à une méthode fondée sur le risque pour contrer les menaces terroristes liées à l'utilisation des systèmes d'aéronefs non habités, dans la mesure où certaines contre-mesures peuvent présenter un risque de sécurité équivalent, voire supérieur à celui posé par les opérations terroristes impliquant des systèmes d'aéronefs non habités.

Bonne pratique n° 19 : Mettre en place des stratégies de gestion et d'atténuation du risque d'incidents liés aux systèmes d'aéronefs non habités.

Aucune stratégie ne peut garantir une sécurité totale face à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités. Par conséquent, les États devraient élaborer des stratégies appropriées et spécifiques de gestion du risque afin d'atténuer l'impact des incidents impliquant des systèmes d'aéronefs non habités.

L'existence de protocoles d'urgence destinés aux différents acteurs, y compris les protocoles d'évaluation précoce de la situation est une condition cruciale pour préparer la réponse la plus efficace possible à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités. Il est fondamental que l'ensemble des acteurs appelés à répondre à un incident impliquant des systèmes d'aéronefs non habités, au niveau national et local, aient reçu une formation adéquate leur permettant de traiter les aspects particuliers de ce type d'incidents. En particulier, les États devraient déterminer comment sécuriser l'espace aérien au-dessus de zones très fréquentées le plus rapidement possible après la survenue d'un incident impliquant un système d'aéronef non habité. La stratégie de gestion de crise est d'une importance capitale pour protéger les aéroports et d'autres sites majeurs accueillant le public, parfois particulièrement vulnérables aux attaques par des systèmes d'aéronefs non habités.

Lors de l'élaboration de ces protocoles, les États devraient examiner les stratégies de crise et d'atténuation déjà en place pour traiter d'autres menaces relatives à la sécurité et à la sûreté publiques. Ces stratégies peuvent servir de modèles pour la conception de protocoles et de stratégies applicables aux urgences impliquant des systèmes d'aéronefs non habités. Néanmoins, les États devraient veiller à adapter ces stratégies de gestion de crise aux particularités spécifiques de la menace posée par les systèmes d'aéronefs non habités.

Bonne pratique n° 20 : Concevoir et mettre en œuvre des règlements et des politiques permettant d'effectuer des enquêtes rapides et complètes, d'engager des poursuites efficaces et d'imposer des sanctions appropriées suite à l'utilisation à des fins terroristes de systèmes d'aéronefs non habités.

Si la prévention de l'utilisation à des fins terroristes de systèmes d'aéronefs non habités est une question cruciale, il est également essentiel que les États prévoient des règlements et des politiques permettant d'enquêter efficacement sur les incidents dus à ces systèmes et de prendre des mesures coercitives si nécessaire. Il est crucial que les enquêtes soient lancées immédiatement après l'incident afin de déterminer si des preuves viennent corroborer l'intention terroriste, si l'incident a une nature criminelle ayant d'autres causes ou s'il n'est dû qu'à la négligence ou à une activité criminelle sans lien avec le terrorisme. Si la visée criminelle ou l'intention de troubler l'ordre public sont démontrées, les enquêtes devraient déboucher sur des poursuites effectives et rapides et, en cas de culpabilité reconnue, sur une sanction ou une peine à l'encontre des auteurs reconnus. Même s'il nécessite dans certains cas de modifier la législation nationale, l'engagement systématique de poursuites peut avoir un effet dissuasif chez certains acteurs terroristes ou chez des individus qui enfreignent la réglementation sur les contrôles des exportations. Les enquêtes civiles sont également nécessaires pour s'assurer que les opérateurs négligents ou mal informés prennent connaissance de leurs obligations et fassent l'objet, si nécessaire, de mesures d'exécution civile afin de décourager de futures infractions. Des sanctions devraient également être prononcées à l'encontre des fabricants, des vendeurs et des exportateurs de systèmes d'aéronefs non habités qui enfreignent la réglementation nationale, comme cela est indiqué dans la Bonne pratique n° 14.

L'octroi de licences d'exploitation, les exigences en matière d'enregistrement et la réglementation sur les contrôles à l'exportation, tels que décrits dans les Bonnes pratiques n° 17 et n° 23, sont de nature à faciliter la recherche des auteurs de crimes ou d'infractions ; de même, les systèmes électroniques

d'identification à distance peuvent aider les services de détection et de répression à analyser les profils de vol ; toutefois, la possibilité d'utiliser des systèmes d'aéronefs non habités fabriqués de manière artisanale ou manœuvrés à partir de modèles en vente libre permet dans certains cas aux terroristes de contourner ces dispositions. Les enquêtes devraient par ailleurs être conduites par des enquêteurs spécifiquement formés et versés dans la technologie des systèmes d'aéronefs non habités, en procédant de manière rapide, efficace et appropriée car l'utilisation de ces systèmes peut n'être qu'un volet d'une stratégie d'agression à plus grande échelle. Plus les faits sont établis tôt, plus les États disposent de temps pour élaborer une réponse appropriée.

Les enquêtes devraient également être menées de manière à permettre aux organismes chargés de l'application de la loi d'identifier le réseau plus vaste à l'origine de l'attaque par des systèmes d'aéronefs non habités. Dans bien des cas, voire dans la plupart des cas, 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° 21 : Mettre en place un processus d'examen périodique des réglementations et des politiques et les réviser si nécessaire.

Les règlements et les politiques en matière de systèmes d'aéronefs non habités peuvent manquer d'efficacité ou se révéler obsolètes à mesure que les évolutions technologiques rendent le cadre existant inapplicable. Par exemple, il deviendra peut-être nécessaire d'élargir la portée des règlements et des politiques afin de couvrir des systèmes d'aéronefs non habités qui n'étaient pas soumis à réglementation jusqu'alors en raison de leur petite taille et qui possèdent désormais des fonctionnalités enrichies, ou des systèmes au sol ou souterrains sans conducteur à mesure que ces technologies évoluent. Par conséquent, les États devraient mettre en place un processus d'examen périodique des règlements et des politiques, et les reconduire ou les réviser suivant les cas.

Le processus de révision devrait reposer sur le partage continu d'expériences de l'ensemble des parties prenantes, à l'échelle nationale et, le cas échéant, internationale et régionale, en prenant en compte les évolutions technologiques. Les règlements devenus manifestement inefficaces, inapplicables, peu pratiques ou disproportionnés devraient être révisés ou abrogés. De même, les États devraient réviser les règlements devenus obsolètes par suite des évolutions technologiques.

IV. Élaboration de contre-mesures tactiques et de solutions techniques

Bonne pratique n° 22 : Mettre en œuvre des mesures de protection visant à atténuer les vulnérabilités.

La vulnérabilité aux attentats impliquant des systèmes d'aéronefs non habités est élevée en l'absence de mesures de protection. Par conséquent, les États devraient mettre en œuvre diverses mesures de protection contre les attentats impliquant des systèmes d'aéronefs non habités, dont la première consiste à accorder les autorisations nécessaires aux autorités compétentes. Les États peuvent concevoir leurs mesures de protection en se basant sur les évaluations du risque et des vulnérabilités telles que décrites dans les Bonnes pratiques n° 1 et n° 3. Les sites identifiés lors de ces évaluations comme étant à haut risque devront être traités en priorité, mais les États devraient également

s'efforcer de protéger d'autres cibles (civiles), en particulier diverses manifestations publiques et les grands rassemblements.

Lors de la mise en œuvre des mesures de protection, les États devraient prendre en compte la nature du site à protéger, son emplacement, son objet et l'utilisation qui en est prévue, ainsi que l'impact que le recours à une mesure visant spécifiquement à contrer des systèmes d'aéronefs non habités peut avoir sur la sécurité. Une mesure appropriée et efficace sur des sites distants peut se révéler extrêmement dangereuse si elle est appliquée dans l'espace aérien d'un aéroport ou d'une zone urbaine fortement peuplée. Il n'existe pas de solution applicable en toutes situations. Les systèmes préventifs sont aussi des contre-mesures envisageables, sous forme de barrières physiques (par exemple, vitrages résistants ou filets de protection), de concepts de sécurité préventive et de protocoles d'urgence tels que les décrit la Bonne pratique n° 19.

Lors des différentes étapes de la lutte contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, les États devraient adopter une méthode à plusieurs niveaux en recourant aux contre-mesures appropriées. Les États devraient commencer par une évaluation complète des types de contre-mesures techniques les plus efficaces suivant plusieurs scénarios spécifiques (par exemple, à proximité des aéroports, au-dessus d'un grand rassemblement public).

Bonne pratique n° 23 : Mettre en place des méthodes de détection et différencier les utilisations légitimes des utilisations à des fins terroristes de systèmes d'aéronefs non habités.

Les études sur le sujet prévoient une augmentation exponentielle des utilisations de systèmes d'aéronefs non habités par le grand public et par le secteur privé. Les États devraient prioriser la mise au point de solutions techniques et de protocoles permettant aux autorités et aux organismes compétents de détecter en temps voulu et de faire rapidement la différence entre les utilisations légitimes, criminelles et à des fins terroristes de systèmes d'aéronefs non habités. Cet aspect est fondamental car la détection précoce des systèmes d'aéronefs non habités suspects laisse davantage de temps aux autorités compétentes pour élaborer une réponse appropriée.

Par conséquent, les États pourraient utiliser une gamme variée d'outils de détection. À l'heure actuelle, le recours aux systèmes radar, scanneurs de radiofréquences, systèmes électro-optiques et caméras infrarouges et capteurs acoustiques, conjugué à l'observation humaine de l'espace aérien, éventuellement soutenue par l'intelligence artificielle, devrait permettre, suivant les capacités de chaque système et les circonstances, de surveiller la totalité de l'espace aérien à des fins de détection précoce des systèmes d'aéronefs non habités. Compte tenu des facteurs environnementaux, des capacités des systèmes d'aéronefs non habités et des failles dont font preuve certains dispositifs de détection, il est peu probable qu'une méthode à capteur unique suffise à assurer la couverture requise.

Les États devraient également mettre en place des méthodes permettant d'identifier les systèmes d'aéronefs non habités suspects. Une solution technique prometteuse, similaire à ce qui se fait déjà avec d'autres systèmes d'aéronefs, consiste à doter chaque système d'aéronef non habités d'un identifiant numérique unique, ce qui permet aux services chargés de l'application de la loi et autres organismes compétents de connaître l'origine des systèmes d'aéronefs non habités et d'identifier leurs propriétaires enregistrés. Les règlements peuvent imposer l'enregistrement auprès des autorités nationales de tout système d'aéronef non habité dépassant une taille définie, et imposer aux systèmes d'émettre leur numéro d'enregistrement, leur vitesse et leur position de vol. Grâce à cette méthode les autorités sont averties de toute présence de systèmes d'aéronefs non habités dans l'espace aérien et peuvent concentrer leurs ressources sur ceux qui ne se conforment pas aux protocoles d'identification à distance ou qui font l'objet d'un signalement en raison des informations qu'ils

émettent. Toutefois, l'ensemble des technologies utilisées pour la gestion du trafic des aéronefs non habités ne présentent pas la même efficacité au regard de la sécurité. Les États devraient donc évaluer et améliorer si besoin l'efficacité des technologies de détection lorsqu'elles sont utilisées pour la détection de systèmes d'aéronefs non habités exploités à des fins terroristes.

L'établissement et la surveillance des zones d'exclusion aérienne et le recours à la géo-détection et aux barrières géolocalisées à proximité des infrastructures sensibles, ainsi que l'application de restrictions claires à l'exploitation comme les décrit la Bonne pratique n° 17 devraient également permettre l'identification précoce des systèmes d'aéronefs non habités non conformes susceptibles d'être manœuvrés par des terroristes. Le tracé des zones d'exclusion aérienne pourrait même être intégré dans la programmation des systèmes d'aéronefs non habités avant leur mise en vente. À cet égard, les États devraient instaurer une collaboration active avec les fabricants privés de systèmes d'aéronefs non habités, comme le recommande la Bonne pratique n° 14, et leur fournir les données nécessaires.

Bonne pratique n° 24 : Concevoir et mettre en œuvre des contre-mesures cinétiques et non cinétiques pour lutter contre les utilisations détournées des systèmes d'aéronefs non habités.

La conception de contre-mesures efficaces pour lutter contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités en est actuellement à ses débuts et reste très fragmentaire. Certaines contre-mesures ont été conçues dans un contexte militaire et n'ont pas été évaluées en vue d'une utilisation sécurisée dans un contexte civil. L'absence de contre-mesures conçues et évaluées à cette fin expose des sites par ailleurs bien protégés à d'éventuelles attaques aériennes. Par conséquent, les États devraient concevoir, tester et mettre en œuvre des contre-mesures efficaces.

Le secteur privé à mis au point un large éventail de contre-mesures, faisant appel à de très nombreuses technologies pour détecter et contrer les utilisations à des fins terroristes de systèmes d'aéronefs non habités. Ainsi, lors de leur évaluation des contre-mesures, les États devraient éviter de « réinventer la roue » et travailler en étroite collaboration avec le secteur privé afin de déterminer quelles sont les solutions les plus adaptées à leur situation. Néanmoins, ceci ne veut pas dire que les États devraient se reposer sur le seul secteur privé. Les États devraient également améliorer et normaliser leurs propres capacités de recherche et de développement, comme le conseille la Bonne pratique n° 8, afin de tester et de vérifier les technologies du secteur privé et, chaque fois que nécessaire, les améliorer ou mettre au point leurs propres contre-mesures. Afin d'éviter toute duplication des efforts, les États devraient également partager avec d'autres États leurs informations sur les mesures les plus efficaces, éventuellement par le biais d'organisations internationales et régionales comme le mentionnent les Bonnes pratiques n° 9 et n° 12.

En règle générale, les contre-mesures cinétiques et non cinétiques ne devraient pas être considérées comme pouvant se substituer aux stratégies de prévention et d'atténuation (par exemple, le dialogue avec le grand public comme le décrit la Bonne pratique n° 15 ; les règlements et les politiques de prévention comme les décrit la Bonne pratique n° 17 ; les protocoles d'urgence efficaces et les capacités d'enquête comme les décrivent les Bonnes pratiques n° 19 et n° 20). Par rapport aux technologies des contre-mesures, les technologies de détection et les stratégies d'atténuation engendrent un niveau moindre de risque pour l'environnement d'exploitation, c'est-à-dire la sécurité de l'espace aérien et les réseaux de communications, et leur utilisation devrait donc être privilégiée. Néanmoins, si besoin est, les États devraient également être prêts à utiliser des contre-mesures efficaces.

Les contre-mesures se répartissent généralement en méthodes cinétiques et non cinétiques. Parmi les contre-mesures cinétiques figurent : l'utilisation de lance-filets ; les projectiles tactiques ; les

armes anti-aériennes ou d'autres systèmes d'aéronefs non habités visant à détruire, à capturer ou à intercepter tout système d'aéronef non habité suspect. Parmi les contre-mesures non cinétiques figurent : la prise de contrôle du système d'aéronef non habité via son protocole de communication ; le brouillage des radiofréquences ou du système global de navigation par satellite ; la destruction par des armes à haute puissance (lasers, armes à micro-ondes, ondes électromagnétiques, etc.) et à ultrasons. Pour obtenir la protection la plus efficace, il conviendrait dans la mesure du possible de regrouper ces mesures au sein d'un système unique ou de les utiliser en tant qu'éléments d'une capacité d'action intégrée. La sélection de la contre-mesure à utiliser dans un environnement particulier doit se faire en fonction de son efficacité attendue face à la menace d'une utilisation à des fins terroristes de systèmes d'aéronefs non habités ainsi que des capacités d'atténuation des éventuels impacts négatifs résultant de son application. L'atténuation doit porter sur les effets collatéraux que la contre-mesure peut avoir sur les personnes, le spectre des services de radiocommunication, les infrastructures et la réputation, comme le décrit plus en détail la Bonne pratique n° 26.

Lorsque cela n'a pas encore été fait, les États devraient mettre en place des procédures accélérées pour évaluer en détail l'efficacité des contre-mesures et leur pertinence dans différents environnements. Cela recouvre aussi l'évaluation de l'efficacité contre les scénarios d'« essaims de drones » mentionnés dans la Bonne pratique n° 1.

Afin que les contre-mesures cinétiques et non cinétiques soient appliquées en toute sécurité, les États devraient fournir les instructions appropriées et dispenser des formations théoriques et pratiques, dans des conditions réalistes, à l'ensemble des autorités chargées de leur déploiement. Cela comprend des formations et des exercices conjoints avec les autorités locales, comme le décrit la Bonne pratique n° 10.

Enfin, les États devraient également soutenir les initiatives du secteur privé ou rendre obligatoire la prise de mesures par ce secteur en vue de prévenir efficacement le piratage de systèmes d'aéronefs non habités prévus pour une utilisation bénéfique ou récréative, en mettant en place des dispositifs robustes de protection contre les prises de contrôle illicites de ces systèmes.

Bonne pratique n° 25 : Mettre en place une procédure d'examen périodique des contre-mesures et les adapter aux évolutions des technologies et des tactiques terroristes.

Comme ce Mémorandum l'a maintes fois fait observer, les technologies des systèmes d'aéronefs non habités connaissent une évolution rapide. De la même manière que les États devraient actualiser en permanence leurs évaluations du risque à la lumière de ces évolutions, ils devraient également s'assurer que les contre-mesures suivent le rythme de ces évolutions et de la montée en puissance systémique des technologies opérant les aéronefs non habités.

Ce processus d'examen devrait être permanent et confié à des évaluateurs du secteur gouvernemental ou à d'autres entités (par exemple, des secteurs universitaire ou privé) dotés des compétences et de l'expérience technologique requises. Le but de l'évaluation devrait être d'identifier, de classer et d'analyser les évolutions pertinentes des technologies en lien avec les systèmes d'aéronefs non habités ainsi que les domaines d'activités interconnectés pouvant avoir un impact sur les possibilités d'exploitation de ces systèmes par des terroristes. Ce processus devrait aussi examiner tout changement observable et potentiel des *modi operandi* des terroristes et chercher à déterminer si les contre-mesures en place sont suffisamment robustes pour contrer les utilisations émergentes et prévisibles de systèmes d'aéronefs non habités à des fins terroristes. Si les contre-mesures se révèlent potentiellement inefficaces, les États devraient les adapter en conséquence ou

concevoir de nouvelles contre-mesures plus efficaces en faisant appel au cadre décrit dans la Bonne pratique n° 24.

Afin d'identifier, d'analyser et de réagir aux évolutions technologiques, les États devraient collaborer avec un large éventail d'intervenants. Parmi ceux-ci on peut citer les technologues de premier plan, les experts, les praticiens spécialisés et les institutions scientifiques. Le secteur privé peut contribuer utilement au processus d'examen et d'élaboration de contre-mesures efficaces et à la pointe du progrès. Les comparaisons avec les politiques d'autres pays et la collaboration en la matière peuvent se révéler extrêmement efficaces pour faire ressortir de nouvelles contre-mesures et stratégies.

Bonne pratique n° 26 : Évaluer les effets négatifs potentiels des contre-mesures sur les infrastructures ainsi que sur les biens, la vie privée et la sécurité des personnes, et prendre des dispositions pour les atténuer.

À chaque étape de la lutte contre l'utilisation à des fins terroristes de systèmes d'aéronefs non habités, les États devraient prendre en compte et essayer d'atténuer ses conséquences négatives sur les infrastructures, la société civile et les biens, la vie privée et la sécurité des personnes. En particulier, le brouillage peut avoir un impact important sur les systèmes d'information, les réseaux d'urgence, les réseaux de communication, les manœuvres d'aéronefs habités ou non habités, les infrastructures des services de navigation, les systèmes de géolocalisation (GPS) et les réseaux de transport. Les États devraient évaluer ces effets collatéraux potentiels et s'abstenir de recourir à des contre-mesures aux effets disproportionnés. Afin d'appréhender les effets collatéraux potentiels, les États devraient travailler en collaboration avec l'ensemble des intervenants mentionnés dans la Section II. Certains organismes et pays chargés d'assurer la sécurité de manifestations publiques à haute visibilité, ainsi que la sécurité de l'aviation et d'autres services critiques tels que les interventions et transports d'urgence ont déjà consacré du temps et des ressources à l'exploration de différents scénarios et devraient faire partie des intervenants associés aux discussions futures sur le sujet.

Les autorités compétentes de l'aviation, les prestataires de services de navigation aérienne et d'autres organismes compétents chargés de la sécurité de l'aviation ont clairement spécifié que les États doivent faire preuve de la plus grande prudence lorsqu'ils envisagent de contrer des systèmes d'aéronefs non habités à proximité des aéroports ou des couloirs de vol. Les mesures interférant avec les systèmes de sécurité des avions ou avec l'infrastructure des services de navigation au sol peuvent occasionner des risques sécuritaires plus graves que la menace potentielle posée par des systèmes d'aéronefs non habités errants.

Il est indispensable que les États procèdent à l'évaluation préalable des impacts potentiels des contre-mesures envisagées, et qu'ils en atténuent, dans la mesure du possible, les effets collatéraux et les répercussions négatives en termes d'exploitation, telles que par exemple, s'agissant des aéroports, la fermeture ou la déviation du trafic aérien. Par exemple, si les contre-mesures interfèrent avec certaines fréquences particulières, celles-ci ne devraient pas être utilisées pour les transmissions sensibles ou d'urgence, ou bien les contre-mesures ne devraient pas être appliquées dans cet environnement particulier ; les États devraient effectuer des évaluations du risque pour prendre en compte ces considérations. Lorsqu'ils lancent des contre-mesures susceptibles d'avoir des conséquences imprévues sur des segments de la société civile, les États devraient faire en sorte de coordonner leur réponse avec un organisme compétent (par exemple, les autorités compétentes de l'aviation, les prestataires de services de navigation aérienne et les organismes régissant la sécurité et les communications de l'aviation) afin d'atténuer au maximum ces conséquences.

Conclusion

Les terroristes ont exploité à maintes reprises les capacités des systèmes d'aéronefs non habités à lancer des attaques et d'autres opérations lors de conflits armés. Il ne fait guère de doute qu'ils tenteront également d'utiliser des systèmes d'aéronefs non habités en dehors du contexte des conflits armés. Afin de se prémunir contre cette menace croissante, les États devraient instaurer des cadres juridiques et politiques puissants à l'échelle nationale et mettre en œuvre des mesures de détection et d'atténuation efficaces. Le *Mémorandum de Berlin sur les bonnes pratiques pour contrer l'utilisation à des fins terroristes de systèmes d'aéronefs non habités* a pour but de fournir aux gouvernements des orientations sur la mise en place des mesures nécessaires de prévention et de réponse face à l'utilisation de systèmes d'aéronefs non habités par des terroristes. Le Mémorandum peut également guider les gouvernements dans la conception et la mise en œuvre des règlements et des protocoles requis pour faciliter et rendre efficaces la gestion de crise et la réalisation d'enquêtes après un incident impliquant des systèmes d'aéronefs non habités.

Cette initiative du GCTF et les bonnes pratiques qui en résultent devraient marquer le début seulement des efforts déployés par les États pour contrer la menace posée par l'utilisation à des fins terroristes de systèmes d'aéronefs non habités. Il est crucial que les États continuent à coopérer entre eux et avec les intervenants tiers. Par leur vigilance ininterrompue, les États peuvent minimiser le risque que représente l'utilisation à des fins terroristes de systèmes d'aéronefs non habités tout en optimisant les avantages qu'apporte la technologie de ces systèmes pour améliorer nos économies et nos sociétés.