



INTERPOL

# CADRE D'INTERVENTION EN CAS D'INCIDENT LIÉ À UN DRONE

À l'intention des premiers intervenants  
et des professionnels de la criminalistique numérique



janvier 2020

Ce document a été élaboré par le Laboratoire de criminalistique numérique du Centre d'innovation d'INTERPOL à Singapour.

Les questions, suggestions et commentaires peuvent être envoyés à l'adresse suivante :

Complexe mondial INTERPOL pour l'innovation  
18 Napier Road  
Singapour 258510

E-mail : [dfi@interpol.int](mailto:dfi@interpol.int)

Tél. : +6565503462

© Complexe mondial INTERPOL pour l'innovation, 2019

# AVANT-PROPOS DU SECRÉTAIRE GÉNÉRAL D'INTERPOL CADRE D'INTERVENTION EN CAS D'INCIDENT LIÉ À UN DRONE

Les drones deviennent de moins en moins coûteux à mesure que la technologie qui les soutient se développe. Leur utilisation est donc en hausse, non seulement à des fins récréatives et commerciales, mais aussi criminelles.

Cela crée inévitablement de sérieux défis pour la communauté mondiale des services chargés de l'application de la loi. Les drones font aujourd'hui partie de l'environnement du travail de police, et ils ne pourront à l'avenir que prendre de l'ampleur et avoir un impact croissant.

Malgré cela, de nombreux fonctionnaires chargés de l'application de la loi ont encore une connaissance et une compréhension insuffisantes des technologies qui composent ces appareils. Lorsqu'ils sont utilisés à des fins malveillantes, les drones représentent une menace importante pour la sécurité et la sûreté de la population. Il est donc primordial que les policiers disposent des connaissances et de la formation nécessaires pour intervenir efficacement et en toute sécurité en cas d'incident lié à ces appareils. De plus, les drones renferment des données précieuses qui, pour servir de preuves dans le cadre d'une enquête, doivent être extraites et analysées.

INTERPOL a donc fait appel aux spécialistes qui, dans les services chargés de l'application de la loi, le secteur privé et les milieux universitaires du monde entier, possèdent une expertise dans le domaine des drones. Ce sont eux qui ont permis l'élaboration du « Cadre INTERPOL d'intervention en cas d'incident lié à un drone – À l'intention des premiers intervenants et des professionnels de la criminalistique numérique ».

Ce document, conçu comme un outil de référence pour la communauté mondiale des services chargés de l'application de la loi, est l'illustration des efforts continus menés par INTERPOL pour promouvoir l'innovation et encourager les bonnes pratiques dans ses pays membres.

Ce Cadre s'inscrit dans l'engagement que nous avons pris – qui est de contribuer à l'avènement d'un monde plus sûr, et je tiens à remercier toutes les personnes qui ont participé à son élaboration.



Jürgen Stock  
Secrétaire Général d'INTERPOL

## LETTRE DE LA DIRECTRICE DU CENTRE D'INNOVATION D'INTERPOL

Partout dans le monde, de nombreuses activités criminelles se développent et prennent l'ampleur de menaces planétaires en s'appuyant sur les progrès technologiques et le caractère sans frontière de notre monde interconnecté. Nous assistons également à l'émergence de formes de criminalité jusqu'ici inconnues des services chargés de l'application de la loi. Ces évolutions ajoutent de la complexité à une situation déjà difficile.

C'est dans ce contexte qu'INTERPOL a créé en 2017 à Singapour un Centre d'innovation, destiné à promouvoir l'innovation au sein de la communauté mondiale des services chargés de l'application de la loi. Dans ce Centre, le Laboratoire de criminalistique numérique a pour mission de développer la formation sur les technologies innovantes et d'accroître les capacités en matière de criminalistique numérique au sein des pays membres d'INTERPOL.

Je suis convaincue que les tâches des laboratoires de criminalistique numérique représentent un volet essentiel du travail de police, en particulier lorsqu'il est question d'enquêter sur des infractions comme des incidents liés à des drones. De fait, les professionnels de la criminalistique numérique sont obligés de constamment se former et développer leurs connaissances, surtout dans le contexte de l'émergence de technologies innovantes comme les drones.

Le Laboratoire de criminalistique numérique organise donc chaque année depuis trois ans des réunions du Groupe d'experts sur les drones, au cours desquelles des spécialistes des services chargés de l'application de la loi, de l'industrie et des milieux universitaires partagent des informations, des connaissances et des bonnes pratiques au sujet des drones. Ce réseau mondial d'experts procure de nombreux avantages et apporte une aide efficace aux pays membres de notre organisation. Je suis heureuse de vous présenter le Cadre INTERPOL d'intervention en cas d'incident lié à un drone – À l'intention des premiers intervenants et des professionnels de la criminalistique numérique, fruit de la collaboration de tous les instants avec la communauté des experts en drones.

Ce Cadre donne une vue d'ensemble des drones et équipements associés, et fournit des conseils qui s'adressent d'une part aux premiers intervenants gérant les incidents avec les drones, et d'autre part aux professionnels de la criminalistique numérique qui recueillent, examinent, analysent et présentent des éléments de preuve numériques sur les drones. Il contribuera, on l'espère, à combler les lacunes en matière de connaissance des drones qui existent au sein de la communauté mondiale des services chargés de l'application de la loi, ainsi qu'à accroître les capacités de ces services – en particulier les premiers intervenants et les professionnels de la criminalistique numérique – à réagir efficacement et en toute sécurité en cas d'incident lié à un drone.

Dans l'espoir de créer une dynamique pour permettre au domaine de la criminalistique numérique de devenir un volet important et solide du travail de police, le Centre d'innovation d'INTERPOL s'attachera à insuffler un esprit d'innovation dans les activités des laboratoires de criminalistique numérique des pays membres, dans le but de relever les défis complexes de la sécurité au niveau mondial.



Anita Hazenberg  
Directrice du Centre d'innovation d'INTERPOL



## Remerciements

Le présent Cadre INTERPOL d'intervention en cas d'incident lié à un drone est le fruit de la contribution de nombreuses parties prenantes. INTERPOL tient tout d'abord à remercier les participants au Groupe d'experts international sur les drones, qui en ont inspiré l'idée. En novembre 2018, six pays et quatre agences des États-Unis se sont réunis à Denver pour débattre des défis et des difficultés que rencontrent les services chargés de l'application de la loi lorsqu'ils doivent gérer un incident lié à un drone. De cette réunion est né le présent Cadre qui, on l'espère, aidera les services chargés de l'application de la loi des pays membres d'INTERPOL à faire face à ce type d'incident.

Ce document reprend également certains fondements de la gestion et du traitement des scènes de crime tirés du « Crime Scene Responder Guide » publié par le *National Institute of Justice* des États-Unis.

INTERPOL tient ensuite à exprimer des remerciements particuliers à Steve Watson, l'organisateur de l'atelier INTERPOL sur l'intervention et l'examen criminalistique numérique dans le contexte des drones, qui a servi de champ d'étude en vue de l'élaboration du présent Cadre. Au cours de cet atelier, neuf pays membres d'INTERPOL ont en effet travaillé sur la structure et le contenu de ce document, afin qu'il puisse répondre aux besoins de tous.

Nous souhaitons également remercier : Harry Blackie, de l'Université de Galles du Sud, pour ses informations sur les emplacements des fichiers de données sur les drones provenant des ensembles de données recueillis par Steve Watson ; Matt Service pour son « Introduction aux drones » utilisée comme source d'informations pour le présent document ; enfin, Dronelogbook.com pour nous avoir autorisés à inclure leur diagramme sur la structure d'un drone.

Enfin, nous tenons à exprimer notre gratitude aux réviseurs spécialisés, qui ont été d'une grande aide en apportant de précieuses idées et des points de vue supplémentaires, en fournissant des informations complémentaires et en contribuant à la touche finale du document, à savoir :

Alexandra Clare Alder, Jamie Allan, Priscilla Cabuyao, Christopher Church, Taurean Dennis, Greg Dominguez, Albert Drijfhout, Daniel Halliwell, Graeme Horsman, Bruce Keeble, David Kovar, Alan McConnell, Alan McDevitt, Joseph Majersky, Geoff Moore, Michal Naglowski, Vincent Olsthoorn, Dale Richards, Fahad E Salameh, Alan Tan et Antonio Sousa Lamas.

Nous profitons de cette occasion pour remercier la communauté des experts en drones et les professionnels des services chargés de l'application de la loi qui, même s'ils ne sont pas cités, ont participé à la conception et l'élaboration de ce Cadre.

TABLE DES MATIÈRES	Page
<b>AVANT-PROPOS DU SECRÉTAIRE GÉNÉRAL D'INTERPOL.....</b>	<b>3</b>
<b>LETTRE DE LA DIRECTRICE DU CENTRE D'INNOVATION D'INTERPOL .....</b>	<b>4</b>
<b>Remerciements .....</b>	<b>5</b>
<b>1. Introduction .....</b>	<b>11</b>
1.1 <b>Objet du document .....</b>	<b>11</b>
1.2 <b>Public visé .....</b>	<b>11</b>
1.3 <b>Champ d'application.....</b>	<b>11</b>
<b>2. Présentation générale des drones .....</b>	<b>11</b>
2.1 <b>Les drones dans le monde d'aujourd'hui .....</b>	<b>11</b>
2.2 <b>Incidents liés à des drones .....</b>	<b>12</b>
2.3 <b>Catégories de drones .....</b>	<b>13</b>
2.4 <b>Composants des drones.....</b>	<b>14</b>
2.4.1 <i>Composants matériels .....</i>	<i>14</i>
2.4.2 <i>Logiciel.....</i>	<i>15</i>
2.5 <b>Charges utiles des drones .....</b>	<b>16</b>
2.6 <b>Les drones et équipements associés en tant que sources d'éléments de preuve .....</b>	<b>17</b>
2.7 <b>Données fournies par les drones .....</b>	<b>19</b>
2.7.1 <i>Types de données .....</i>	<i>19</i>
2.7.2 <i>Accès à différents supports de stockage des données.....</i>	<i>20</i>
2.7.3 <i>Ce qu'il faut savoir sur les données lors des enquêtes concernant des drones .....</i>	<i>21</i>
2.8 <b>Infractions pouvant être commises avec un drone.....</b>	<b>22</b>
2.9 <b>Vue d'ensemble de la législation sur les drones .....</b>	<b>23</b>
2.10 <b>Consignes pour un usage des drones en toute sécurité .....</b>	<b>23</b>
2.11 <b>Exemples de drones et équipements associés.....</b>	<b>26</b>
<b>3. Consignes à l'intention des premiers intervenants.....</b>	<b>31</b>
3.1 <b>Première intervention/Prise d'informations.....</b>	<b>31</b>
3.2 <b>Procédures de sécurité .....</b>	<b>32</b>
3.3 <b>Soins d'urgence .....</b>	<b>33</b>
3.4 <b>Sécurisation et contrôle des personnes et des éventuels éléments de preuve sur la scène .....</b>	<b>34</b>
3.5 <b>Transfert de la gestion de la scène de crime et compte rendu à l'enquêteur chargé de l'affaire .....</b>	<b>34</b>
3.6 <b>Consignation par écrit des actions et des observations .....</b>	<b>35</b>
3.7 <b>Établissement d'un poste de commandement (système de commande d'incident) et envoi de messages.....</b>	<b>35</b>
3.8 <b>Gestion des témoins .....</b>	<b>36</b>
3.9 <b>Évaluation de la scène .....</b>	<b>37</b>
3.10 <b>Délimitation de la scène : repérage, mise en place, protection et sécurisation.....</b>	<b>38</b>
3.11 <b>Inspection de la scène et premiers relevés .....</b>	<b>39</b>

3.12	Prise de notes et tenue d'un registre.....	40
3.13	Saisie d'un drone .....	41
3.14	Déroulement de l'enquête .....	46
3.14.1	<i>Enquête complémentaire</i> .....	48
4.	Présentation générale et principes de la criminalistique numérique.....	48
4.1	Présentation générale .....	48
4.2	Principes des éléments de preuve électroniques .....	49
4.3	Présentation générale d'un laboratoire de criminalistique numérique .....	50
4.3.1	<i>Réception de la demande</i> .....	50
4.3.2	<i>Enregistrement du dossier</i> .....	50
4.3.3	<i>Enregistrement des pièces à conviction</i> .....	51
4.3.4	<i>Photographie des pièces à conviction</i> .....	51
4.3.5	<i>Analyse</i> .....	51
4.3.6	<i>Restitution des pièces à conviction</i> .....	52
4.3.7	<i>Clôture du dossier</i> .....	52
5.	Analyse criminalistique numérique d'un drone.....	52
5.1	Présentation générale .....	52
5.1.1	<i>Les drones et leurs équipements</i> .....	53
5.2	Acquisition .....	53
5.2.1	<i>Méthodes d'extraction des données</i> .....	54
5.2.2	<i>Outils d'extraction</i> .....	55
5.2.3	<i>Format des fichiers d'extraction</i> .....	55
5.2.4	<i>Processus d'extraction</i> .....	56
5.2.6	<i>Autres sources de preuves</i> .....	61
5.3	Examen .....	62
5.4	Analyse .....	62
5.4.1	<i>Procédures d'analyse des traces numériques</i> .....	62
5.5	Présentation.....	65
5.5.1	<i>Recevabilité des preuves électroniques</i> .....	65
5.5.2	<i>Rédaction du rapport</i> .....	66
5.5.3	<i>Témoin expert</i> .....	66
6.	Exemples de données se trouvant sur un drone.....	67
6.1	Journaux de vol .....	67
6.2	Fichiers multimédias.....	67
6.3	Applications mobiles associées .....	68
6.3.1	<i>Application mobile associée aux drones DJI</i> .....	69
6.3.2	<i>Application mobile associée aux drones Parrot</i> .....	70
6.3.3	<i>Application mobile associée aux drones Yuneec</i> .....	72
6.3.4	<i>Application mobile associée à une caméra de drone Yuneec</i> .....	73
6.4	Emplacements de stockage sur les drones.....	75
7.	Outils couramment utilisés pour l'analyse criminalistique des drones .....	75
7.1	Cellebrite/MSAB XRY/Oxygen/CFID .....	75
7.2	CsvView et DatCon [ <a href="http://datfile.net/">http://datfile.net/</a> ] .....	76

7.3	<b>DROP (<i>DRone Open source Parser</i>)</b> [ <a href="https://github.com/unhcfreg/">https://github.com/unhcfreg/</a> ].....	76
7.4	<b>Google Earth Pro</b> [ <a href="https://www.google.co.uk/earth/versions/#download-pro">https://www.google.co.uk/earth/versions/#download-pro</a> ].....	76
7.5	<b>ST2Dash et Dashware</b> [ <a href="https://github.com/ajpierson/st2dash">https://github.com/ajpierson/st2dash</a> ; <a href="http://www.dashware.net/">http://www.dashware.net/</a> ].....	76
7.6	<b>DJI Assistant</b> .....	76
7.7	<b>FTK Imager</b> .....	76
7.8	<b>VLC Player</b> .....	76
8.	<b>Ressources Web utiles</b> .....	77
<b>Annexes</b>	.....	<b>78</b>
<b>Annexe A : Types de drones</b>	.....	<b>78</b>
<b>Annexe B : Compte rendu d'incident lié à un drone par les premiers intervenants</b>	.....	<b>81</b>
<b>Annexe C : Feuille d'enregistrement d'un incident lié à un drone</b>	.....	<b>84</b>
<b>Annexe D : Compte rendu d'examen d'un drone</b>	.....	<b>87</b>
<b>Annexe E : Consignes de sécurité relatives aux batteries LiPo</b>	.....	<b>94</b>
<b>Annexe F : Liste de contrôle du kit d'intervention de base</b>	.....	<b>95</b>
<b>Annexe G : Compétences de base des premiers intervenants et des professionnels de la criminalistique numérique</b>	.....	<b>96</b>
<b>Annexe H : Compétences de base des premiers intervenants</b>	.....	<b>98</b>
<b>Annexe I : Compétences de base des premiers intervenants généralistes</b>	.....	<b>99</b>
<b>Annexe J : Compétences de base des premiers intervenants techniques</b>	.....	<b>100</b>
<b>Annexe K : Compétences de base des premiers intervenants avancés</b>	.....	<b>101</b>
<b>Glossaires</b>	.....	<b>102</b>
<b>Glossaire I : Acronymes utilisés dans l'aviation</b>	.....	<b>103</b>
<b>Glossaire II : Abréviations de termes techniques</b>	.....	<b>105</b>
<b>Glossaire III : Terminologie de la criminalistique numérique appliquée aux drones</b>	.....	<b>106</b>
<b>Glossaire IV : Termes relatifs aux UAV</b>	.....	<b>112</b>

## Liste des figures

Figure 1 : Drone écrasé avec son chargement de drogue.....	12
Figure 2 : Drones récréatifs .....	13
Figure 3 : Drones commerciaux.....	14
Figure 4 : Drones sur mesure .....	14
Figure 5 : Télécommandes .....	17
Figure 6 : Télécommandes sur lesquelles sont fixés des smartphones/tablettes .....	17
Figure 7 : Lunettes immersives.....	18
Figure 8 : Carte mémoire Micro SD.....	18
Figure 9 : Icônes de stockage sur le nuage.....	18
Figure 10 : Éléments de preuve humides.....	19
Figure 11 : Document infographique sur l'usage des drones en toute sécurité établi par l'autorité de l'aviation de Singapour .....	25
Figure 12 : Document infographique sur la classification des véhicules sans pilote établi par l'administration fédérale de l'aviation des États-Unis .....	26
Figure 13 : Télécommande de drone avec écran intégré.....	26
Figure 14 : Vue d'ensemble des composants d'un quadricoptère.....	27
Figure 15 : Vue d'ensemble des composants d'un drone à voilure fixe .....	27
Figure 16 : Télécommande sans écran.....	28
Figure 17 : Télécommande avec support pour smartphone.....	28
Figure 18 : Application mobile de contrôle .....	29
Figure 19 : Planificateur de mission .....	30
Figure 20 : Précautions à prendre avant de s'approcher d'un drone dans le contexte d'un incident.....	43
Figure 21 : Précautions à prendre lors de la manipulation d'un drone .....	44
Figure 22 : Consignes de manipulation d'un drone .....	45
<b>Figure 23 : Consignes de sécurité d'une batterie LiPo .....</b>	<b>45</b>
Figure 24 : Préservation des éléments de preuve numériques .....	45
Figure 25 : Collecte d'éléments de preuve numériques .....	46
Figure 26 : Relevés d'informations sur la scène de l'incident.....	46
Figure 27 : Vue d'ensemble du déroulement d'une enquête .....	47
Figure 28 : Analystes de criminalistique numérique examinant un drone .....	49
Figure 29 : Processus de travail d'un laboratoire de criminalistique numérique .....	50
Figure 30 : Modèle d'analyse criminalistique numérique.....	52
Figure 31 : Drone en cours d'examen .....	54
Figure 32 : Processus d'extraction des données contenues sur les drones et leurs télécommandes	56
Figure 33 : Étiquette d'identification d'un drone.....	56
Figure 34 : Diagramme récapitulatif de l'examen d'un drone .....	60
Figure 35 : Diagramme récapitulatif de l'examen d'une télécommande .....	61
Figure 36 : Autres sources de preuves .....	62
Figure 37 : Télécommande Yuneec .....	74
Figure 38 : Emplacements de stockage des données sur le Typhoon Q500 4K de Yuneec .....	75



## Liste des tableaux

Tableau 1 - Ce qu'il faut savoir sur les données lors des enquêtes concernant des drones .....	21
Tableau 2 - Consignes pour un usage des drones en toute sécurité .....	24
Tableau 3 - Étapes de traitement d'une scène de crime .....	31
Tableau 4 - Procédure de la première intervention/prise d'informations .....	32
Tableau 5 - Procédures de sécurité.....	32
Tableau 6 - Procédure des soins d'urgence .....	33
Tableau 7 - Procédure de sécurisation et de contrôle des personnes présentes sur la scène .....	34
Tableau 8 - Procédure du transfert de la gestion de la scène de crime et du compte rendu à l'enquêteur chargé de l'affaire .....	34
Tableau 9 - Procédure de consignation par écrit des actions et des observations.....	35
Tableau 10 - Procédure d'établissement d'un poste de commandement (système de commande d'incident) et d'envoi de messages .....	36
Tableau 11 - Procédure de gestion des témoins.....	37
Tableau 12 - Procédure d'évaluation de la scène .....	37
Tableau 13 - Délimitation de la scène : repérage, mise en place, protection et sécurisation .....	38
Tableau 14 - Procédure d'inspection de la scène et de réalisation des premiers relevés .....	39
Tableau 15 - Procédure de prise de notes et de tenue d'un registre .....	40
Tableau 16 - Processus de saisie d'un drone.....	41
Tableau 17 - Dangers liés au drone .....	43
Tableau 18 - Les trois éléments à prendre en compte avant de lancer une enquête complémentaire.....	48
Tableau 19 - Principes de base applicables aux éléments de preuve numériques .....	49
Tableau 20 - Types de données stockées sur la télécommande d'un drone .....	53
Tableau 21 - Méthodes pour isoler la pièce à conviction (drone/télécommande) .....	57
Tableau 22 - Dispositifs de stockage sur les drones/télécommandes .....	58
Tableau 23 - Traces numériques pouvant se trouver sur un drone/une télécommande.....	58
Tableau 24 - Critères généraux de recevabilité des preuves électroniques .....	65
Tableau 25 - Emplacements des journaux de vol sur certains drones courants.....	67
Tableau 26 - Emplacements des fichiers multimédias sur certains drones courants .....	67
Tableau 27 - Application mobile DJI Go 4 .....	69
Tableau 28 - Aperçu de l'application mobile Parrot Freeflight .....	70
Tableau 29 - Aperçu de l'application mobile Yuneec Pilot.....	70
Tableau 30 - Aperçu de l'application mobile associée à une caméra de drone Yuneec.....	71

## 1. INTRODUCTION

### 1.1 Objet du document

Ce Cadre INTERPOL d'intervention en cas d'incident lié à un drone, qui s'adresse aux premiers intervenants et aux professionnels de la criminalistique numérique, fournit des lignes directrices sur la façon de gérer les incidents impliquant des drones. Le but est de dispenser des conseils techniques pour gérer et traiter ce type d'incident.

L'objectif de ces lignes directrices est de s'assurer que les pays membres d'INTERPOL disposent des informations nécessaires pour pouvoir faire face du mieux possible à des incidents causés par des drones. Les conseils qui sont fournis doivent être utilisés comme références aux niveaux stratégique et tactique. Ces lignes directrices ont pour seule vocation de servir de modèle aux pays lorsqu'ils mettent en place une intervention. Elles doivent être modifiées ou adaptées en fonction de la législation, des pratiques et des procédures de chaque pays membre, afin de répondre au mieux aux besoins de chacun.

### 1.2 Public visé

Ce Cadre s'adresse aux pays membres d'INTERPOL. Il a été conçu pour deux types de publics : d'une part, les premiers intervenants et les policiers qui assistent aux incidents ; d'autre part, les professionnels de la criminalistique numérique qui traitent les éléments de preuve électroniques après l'incident.

Les procureurs, juges et avocats peuvent aussi tirer parti de ce guide en acquérant une meilleure compréhension des drones et du processus conduisant à des incidents. Il peut leur être utile pour comprendre les affaires liées aux drones et leurs caractéristiques particulières.

### 1.3 Champ d'application

Ce Cadre n'a pas pour but de fixer des limites aux premiers intervenants ou au personnel technique, qui ont pour obligation de respecter le cadre juridique de leur pays. Les conseils donnés ici ne sont pas censés aller à l'encontre de la législation ou des directives nationales.

## 2. PRESENTATION GENERALE DES DRONES

### 2.1 Les drones dans le monde d'aujourd'hui

Les drones connaissent aujourd'hui un large engouement, depuis leur usage par les jeunes à des fins récréatives jusqu'à leur adoption par des malfaiteurs expérimentés pour acheminer des biens illicites. Que l'on s'intéresse à la technologie ou pas, il est impossible d'échapper à l'omniprésence de ces appareils dans la vie de tous les jours : dans les parcs (où ils sont utilisés à titre de loisir), les médias traditionnels, les médias sociaux ou encore les films et les émissions télévisées. L'actualité est régulièrement ponctuée de récits – positifs et négatifs – sur l'utilisation des drones faisant état des opportunités, des risques et des menaces qu'ils peuvent représenter pour les principaux secteurs industriels et pour le grand public.

Le changement d'image auprès du public, la diversification des fabricants et des modèles proposés, la baisse des prix due à la standardisation et les progrès technologiques rapides sont autant de facteurs ayant contribué à l'acquisition massive de drones dans le monde entier. Bien que « drone » soit le terme généralement et régulièrement employé par le grand public et les médias traditionnels, les services chargés de l'application de la loi de nombreux pays utilisent d'autres appellations telles que :

véhicule aérien sans pilote (UAV), système d'aéronef non habité (UAS), petit système d'aéronef non habité (SUAS) et système d'aéronef télépiloté (RPAS). Le présent document emploiera invariablement « drone » et « UAV ».

L'adoption croissante d'UAV à usage récréatif et commercial dans le monde entier signifie que les interactions des forces de police et des services chargés de l'application de la loi avec ces appareils – ainsi qu'avec leurs propriétaires et leurs exploitants – deviendront à l'avenir de plus en plus courantes.

## 2.2 Incidents liés à des drones

De tailles et de formes diverses, les drones peuvent avoir toutes sortes d'utilisations allant de la photographie et la vidéo aériennes au transport de biens d'un endroit à un autre. L'offre de drones et leur usage par le grand public ne cessent de s'accroître depuis quelques années. Le corollaire de cette situation est que ces appareils sont également mis à profit par les malfaiteurs pour commettre des actes illicites tels que : violation de la vie privée, trafic de drogues, actes terroristes et désorganisation des infrastructures critiques. Voici des exemples courants :

- Transport de produits de contrebande dans des zones interdites d'accès comme les prisons ;
- Survol de zones réglementées pour prendre des photos ou des vidéos à usage personnel, ou pour recueillir des renseignements ;
- Menace de perturbation des activités quotidiennes, comme le vol d'un drone au-dessus ou à proximité d'un aéroport.



Figure 1 : Drone écrasé avec son chargement de drogue

Plusieurs incidents impliquant des drones ont eu lieu ces dernières années dans différents pays. Ce fut le cas par exemple en décembre 2018 à l'aéroport de Gatwick, au Royaume-Uni, où un UAV non autorisé a survolé les bâtiments et les pistes. Cet incident a perturbé les activités aéroportuaires pendant environ trois jours, touchant des milliers de personnes et coûtant des millions de livres. Deux autres incidents sont survenus à l'aéroport Changi de Singapour au cours d'une même semaine en juin 2019, entraînant la désorganisation des activités aéroportuaires pendant plusieurs heures, la perturbation d'environ 65 vols et des désagréments pour de nombreux voyageurs.

D'autres incidents liés à des drones ont également frappé ces dernières années de nombreux secteurs et de nombreuses personnes à l'échelle mondiale. Par exemple, au cours du seul premier semestre 2019, des incidents survenus dans des aéroports et des prisons des pays ci-dessous ont été rapportés dans les médias.

### Aéroports :

- Singapour, Angleterre, Irlande, Écosse, Canada, Allemagne, Italie, Doubaï, États-Unis, Mexique, Nouvelle-Zélande et Norvège.

### Prisons :

- États-Unis, Italie, Écosse, Irlande, Angleterre et Canada.

Cela dit, bien que les incidents ci-dessus soient médiatisés, la liste des utilisations potentielles de drones pour commettre et prévenir des infractions est quasiment infinie. À mesure que leur technologie continuera de se développer et que leur prix continueront de baisser, les drones feront de plus en plus partie du paysage, ce qui représentera de nouveaux défis pour la communauté des services chargés de l'application de la loi, depuis les premiers intervenants jusqu'aux spécialistes de la criminalistique numérique.

### 2.3 Catégories de drones

Compte tenu du nombre de drones existant sur le marché ainsi que des larges gammes de prix, il n'est pas facile d'avoir une vision claire des différents types d'UAV disponibles. Les travaux que nous avons menés montrent que les drones peuvent en fait être classés en trois catégories :

#### a) Drones récréatifs

Ces types de drones sont conçus pour les utilisateurs amateurs, ceux qui en font une activité de loisir, et les enfants ; ils coûtent généralement peu cher. Leurs caractéristiques techniques sont minimales et leur coût est inférieur à 23 EUR. Ces appareils sont généralement destinés à un usage en extérieur, et leur durée d'autonomie est très faible. Les drones sont souvent dits « récréatifs » lorsqu'ils pèsent moins de 250 grammes. On en compte aujourd'hui plusieurs milliers sur le marché, disponibles auprès des vendeurs de produits techniques, des magasins de jouets, et d'une pléthore de marchands en ligne.

Dans la mesure où la législation applicable s'appuie non sur les capacités de ces appareils mais sur l'usage auquel ils sont destinés, il n'existe pas de limite supérieure au classement d'un UAV dans la catégorie des drones récréatifs. On y trouve donc des appareils très coûteux, pouvant atteindre des milliers d'euros.



Figure 2 : Drones récréatifs

#### b) Drones commerciaux

Ces types de drones sont conçus pour être utilisés à des fins commerciales. Ils transportent généralement une charge utile correspondant à l'usage pour lequel ils ont été conçus (par exemple, un appareil photo utilisé pour prendre des photos professionnelles, inspecter un site industriel ou effectuer un relevé topographique). Tout comme la catégorie précédente, les drones commerciaux ne sont pas classés en fonction de leurs capacités, mais de l'utilisation qui en sera faite. Par conséquent, même l'UAV le moins coûteux peut être classé dans la catégorie des « drones commerciaux » si son exploitant le destine à un usage commercial. Cela dit, il existe à l'échelle mondiale un grand nombre de fabricants d'UAV conçus principalement pour un usage commercial et non récréatif ; la plupart de ces appareils coûtent plusieurs milliers d'euros.

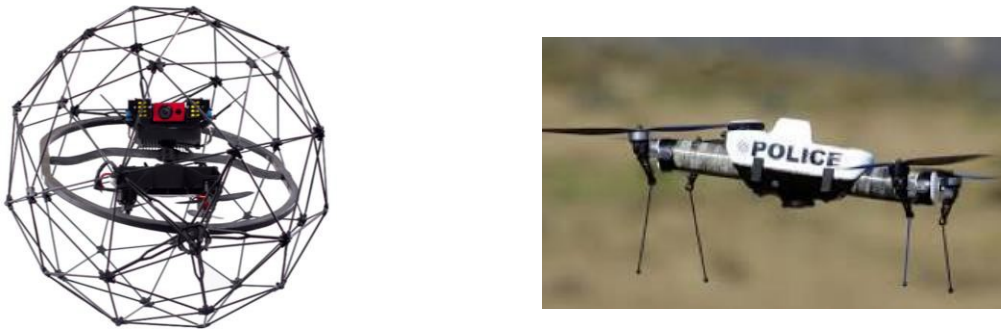


Figure 3 : Drones commerciaux

### c) Drones sur mesure

Les drones sur mesure sont conçus par leur propriétaire, qui achète chaque pièce séparément et les assemble (plutôt que d'acheter un UAV tout prêt dans un magasin). Bien que les drones récréatifs et commerciaux offrent d'excellentes fonctionnalités – en associant un appareil et un logiciel de pilotage prêts à l'emploi –, le marché des drones sur mesure s'est développé à grande vitesse ces dernières années car un large choix de pièces détachées ont fait leur apparition sous forme standardisée, entraînant une baisse des coûts.

Les drones sur mesure permettent à un utilisateur ou un vendeur d'acheter des pièces détachées auprès de différentes sources, puis de construire et de configurer l'appareil en fonction de ses besoins ou de son budget. Les capacités des drones dépendent uniquement de la capacité des pièces disponibles ainsi que des compétences et des connaissances de la personne qui les assemble, or des améliorations exponentielles ont lieu dans les deux domaines.

Ces types de drones peuvent être conçus à très faible coût pour un usage récréatif (par exemple, un jouet pour enfant). Ils peuvent aussi être conçus, configurés et construits par des passionnés et des spécialistes, auquel cas ils égalent en capacités les appareils commerciaux des grandes marques de fabricants et comportent des pièces coûtant des milliers d'euros.

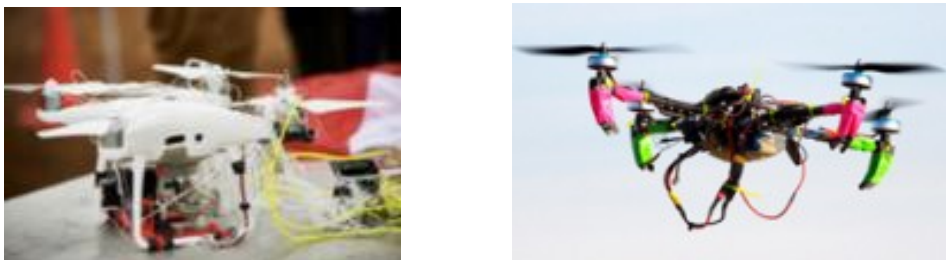


Figure 4 : Drones sur mesure

## 2.4 Composants des drones

Tous les types de drones renferment les deux catégories de composants suivantes.

### 2.4.1 Composants matériels

Les pièces qui composent le fuselage et le dispositif de vol d'un drone peuvent se classer dans les catégories suivantes. Un drone ne renferme pas nécessairement toutes les pièces indiquées ici, mais les catégories sont toujours celles répertoriées ci-dessous :

#### i) Fuselage

Corps du drone renfermant tous les autres composants.



*ii) Contrôleur de vol*

Ce système, utilisé pour le pilotage du drone, permet de stabiliser l'appareil et peut généralement recevoir des instructions d'un émetteur radio. Sur les drones les plus élaborés, le contrôleur de vol peut soit être télécommandé en temps réel, soit être préprogrammé pour des vols en autonomie.

*iii) Moteurs, rotors/hélices/ailerons et variateur de vitesse*

Combinées, ces pièces assurent la portance et la propulsion du drone. Elles existent dans différents modèles, par exemple pour apporter plus de vitesse ou allonger la durée de vol.

*iv) Boîtier de protection*

Ce boîtier protège les moteurs et les hélices (qui sont les composants les plus fragiles d'un drone) contre les collisions et les pertes de contrôle, qui peuvent endommager le système.

*v) Récepteur GPS*

Pas indispensable mais courant sur les appareils de renom, ce composant permet de gérer efficacement la position du drone, le retour au point de départ sans problème et les vols autonomes.

*vi) Récepteur radio (RX)*

Dispositif recevant les instructions envoyées par l'émetteur au sol.

*vii) Émetteur (TX)*

Dispositif permettant à l'exploitant au sol d'envoyer manuellement des instructions au drone.

*viii) Ampoules LED*

Certains drones sont équipés d'ampoules LED (généralement rouges et vertes). Elles peuvent aider le pilote à orienter son appareil et permettre aux autres usagers de l'espace aérien de le repérer.

**2.4.2 Logiciel**

Tous les drones sont équipés d'une application ou d'un logiciel qui sert à commander le système lorsqu'il est en fonctionnement. Si tous les drones à usage récréatif ou commercial sont généralement fournis avec leur propre logiciel ou système de commande préconfiguré, pour les drones sur mesure, en revanche, c'est à la personne qui les assemble de concevoir ou d'intégrer un composant qui fonctionne. Confortant cette tendance, des sites Internet proposent aujourd'hui de nombreux logiciels de gestion de vol et de contrôle au sol au code source ouvert, qui peuvent être téléchargés gratuitement et facilement adaptés pour accomplir toutes sortes de tâches.

Quel que soit le système utilisé ou la façon dont les composants sont configurés, les logiciels rencontrés dans le domaine des drones peuvent être classés en deux grandes catégories :

*a) Logiciel de gestion de vol*

Ce logiciel est installé d'une part sur le contrôleur de vol de l'UAV, et d'autre part sur la télécommande de l'utilisateur. Il sert à contrôler le drone au moment du décollage et de l'atterrissage, ainsi que pendant le vol. Les fonctions généralement assurées par ce logiciel sont le vol du drone, la stabilisation de l'appareil et le pilotage en mode manuel.

*b) Logiciel de contrôle au sol*

Ce logiciel sert à vérifier un plan de vol préétabli et à en concevoir d'autres. Il est généralement utilisé par le pilote pour planifier et préparer un vol lorsque le drone est au sol. Lorsque l'UAV est en vol, ce logiciel permet en outre à des utilisateurs autres que le pilote de le suivre en temps réel, que ce soit directement sur leur ordinateur ou depuis des appareils intelligents (tablettes ou téléphones portables, par exemple).

Bien que très innovants et favorisant le développement des compétences techniques, les drones sur mesure, généralement configurés dans un souci de commodité et de coût plutôt que de sécurité, peuvent accroître les risques et exposer à des dangers. La conséquence est qu'ils risquent d'être dépourvus des fonctionnalités et dispositifs de sécurité de base dont sont dotés un grand nombre des appareils de renom vendus dans le commerce (comme le contrôle d'accès aux zones réglementées, l'évitement d'obstacles et la gestion en toute sécurité des défaillances). En cas d'erreur du pilote ou de dysfonctionnement de l'appareil, ces fonctionnalités garantissent la protection des personnes et des biens.

Si les catégories de drones proposées ici peuvent parfois être difficiles à délimiter – par exemple lorsque des utilisateurs fortunés acquièrent pour un usage récréatif des UAV haut de gamme destinés à un usage commercial –, l'utilisation de cette classification est néanmoins recommandée pour définir les drones et examiner leurs capacités respectives.

## 2.5 Charges utiles des drones

De nombreux types de charges utiles, aux gammes de prix variées, peuvent être transportés par les drones commerciaux. On peut généralement les classer dans les catégories suivantes.

### *a) Appareils photo et vidéo*

Bien que la plupart des UAV intègrent un dispositif de prise de vue, celui-ci est nettement plus élaboré sur les drones à usage commercial et incluent des fonctionnalités comme le mode immersion (FPV), la norme vidéo 4K, le zoom optique pour les inspections et le géomarquage pour les cartes en 3D. Les systèmes de prise de vue plus élaborés peuvent inclure des cardans permettant de maintenir l'appareil photo/vidéo en position droite et stable, afin de produire des images de grande qualité en éliminant les mouvements dus au vol.

### *b) Systèmes thermiques, infrarouges et infrarouges à vision frontale (FLIR)*

Traditionnellement réservés aux appareils haut de gamme, les systèmes d'imagerie thermique peuvent avoir des utilisations variées : recensement agricole, santé et sécurité, application de la loi, recherche et sauvetage. Les systèmes infrarouges peuvent être particulièrement utiles pour permettre aux drones de se diriger efficacement lors de vols de nuit ou dans l'obscurité. Les systèmes FLIR utilisent une caméra thermique qui capte les variations les plus fines du rayonnement infrarouge. Ils peuvent ainsi distinguer les différentes gammes de fréquences, détecter des composés chimiques, et saisir l'emplacement exact des objets et la distance entre eux grâce à la technique de détection et télémétrie par ondes lumineuses (LIDAR).

### *c) Produits à livrer*

L'utilisation des drones en tant que moyens de transport rapides et efficaces est depuis quelques années un domaine d'investissement croissant, l'exemple le plus médiatisé étant celui d'Amazon et de son service Prime Air.

Si les livraisons des commerces et des entreprises pourraient être un créneau d'utilisation massive des drones, le déploiement des applications radio et la mise à profit de la technologie dans le domaine des livraisons pourraient favoriser le développement d'autres secteurs, comme celui de la santé (les UAV transportant sur demande des produits requis de toute urgence, par exemple des défibrillateurs). Cela dit, les drones peuvent aussi être utilisés de façon innovante par les malfaiteurs pour acheminer de la drogue, des armes et autres biens illicites. Ce procédé a été utilisé dans des prisons de plusieurs pays.

#### d) Armes

Les UAV peuvent transporter des armes ou être utilisés eux-mêmes pour conduire des attaques armées. On le voit aujourd'hui régulièrement dans le domaine militaire, où les drones sont choisis comme méthode d'attaque en raison de leur haut degré de précision et du faible risque de perte de vie humaine qu'ils représentent par rapport aux méthodes de combat traditionnelles par l'intermédiaire d'êtres humains. Un UAV de milieu de gamme peut transporter une charge utile de 3 kg pendant 16 minutes à la vitesse de 16 mètres/seconde. Cela équivaut à un véhicule autonome transportant 3 kg d'explosifs à une distance de 16 kilomètres.

#### e) Outils de communication

Il est encore rare de trouver des outils de communication embarqués sur les UAV, mais cela risque de devenir plus courant avec le déploiement des réseaux 5G. Les drones peuvent en effet transporter des outils de communication pouvant servir à espionner, interrompre ou imiter des communications privées légitimes transitant par un réseau sans fil – par exemple en mystifiant des antennes-relais ou des points d'accès sans fil.

## 2.6 Les drones et équipements associés en tant que sources d'éléments de preuve

Contrairement à de nombreux autres appareils électroniques, les drones ont besoin d'autres équipements pour fonctionner correctement, comme les suivants :

#### a) Télécommande

Cet appareil permet de contrôler le drone à distance.



Figure 5 : Télécommandes

#### b) Smartphone/Tablette

Ces appareils permettent de visualiser les photos et vidéos prises par le drone.



Figure 6 : Télécommandes sur lesquelles sont fixés des smartphones/tablettes

*c) Lunettes immersives*

Les lunettes immersives permettent de visualiser les photos et vidéos prises par le drone, ainsi que de contrôler l'engin par des mouvements de tête ou des boutons de commande.



Figure 7 : Lunettes immersives

*d) Cartes mémoire*

Des supports amovibles peuvent être utilisés pour enregistrer les photos et vidéos prises par le drone. Ces supports peuvent aussi contenir des informations sur la trajectoire de vol ainsi que des données EXIF (*Exchangeable Image File*) permettant le géomarkage des photos.

Figure 8 : Carte mémoire Micro SD



*e) Stockage sur le nuage*

Un drone peut utiliser l'appareil mobile qui lui est associé pour stocker des photos ou des vidéos sur le nuage, à l'aide de services comme iCloud ou Google Photos.



Figure 9 : Icônes de stockage sur le nuage

*f) Éléments de preuve humides*

Comme tout objet matériel, un drone et les équipements qui y sont associés peuvent comporter des preuves humides (empreintes, ADN, etc.).



Figure 10 : Éléments de preuve humides

Si le drone est la principale source d'éléments de preuve, il est primordial de sécuriser d'autres sources possibles de preuves (comme la télécommande, le smartphone/la tablette et les cartes mémoire) afin d'obtenir la vision la plus complète possible des événements et de recueillir le plus de renseignements y afférents.

Lors d'un incident lié à un drone, il est important de collecter le plus d'informations possible sur l'incident et les faits connexes (par exemple : identification des principaux témoins, examen des lieux et du contexte). Certains de ces éléments risquent dans un premier temps de paraître superflus, mais ils pourront devenir déterminants à mesure que l'enquête progressera.

## 2.7 Données fournies par les drones

Comme tout appareil ou solution électronique, un drone laisse inévitablement une empreinte numérique (création et stockage de données), que ce soit directement dans le cadre de son utilisation de base ou indirectement (journaux contenant l'historique des utilisations).

### 2.7.1 Types de données

Lorsqu'une enquête est menée au sujet d'un incident lié à un drone, différents types de données peuvent être utilisés :

#### a) Contenus audiovisuels

Dans la plupart des cas, le premier et principal type de données stockées par un drone (à usage récréatif ou commercial) est l'ensemble des photos ou vidéos numériques prises par l'appareil. La plupart des exploitants d'UAV s'efforcent aujourd'hui d'obtenir la meilleure qualité d'image possible afin d'en faire un argument de vente et un avantage commercial vis-à-vis de leurs concurrents. Cela peut se traduire par l'accumulation d'une grande quantité de données et de gros besoins de stockage, même lors de courtes séquences de prise de vues.

#### b) Programmes de vol

Lorsque le système de contrôle du drone permet de planifier des vols à l'avance et offre à l'utilisateur un certain degré d'autonomie, les données correspondantes sont conservées et peuvent être consultées par l'utilisateur pour revoir l'activité passée, répéter un vol planifié ou modifier des programmes de vol existants. Souvent, les données enregistrées pendant le vol puis téléchargées sur un système de contrôle ou une plateforme d'examen des programmes de vol sont volontairement conservées par l'utilisateur pour vérifier et examiner l'usage du drone sur une carte, de manière à suivre son activité et sa progression.



### *c) Autres contenus*

Lorsque des charges utiles sont embarquées sur un drone, il est fort probable aussi qu'elles enregistrent des données, ensuite accessibles à l'utilisateur ou à n'importe quelle organisation. Les types de données varient selon la charge en question, un exemple étant celui des UAV utilisés pour des livraisons de produits. Les données enregistrées renseigneront sur les horaires, les lieux et les résultats de leurs missions.

### *d) Fichiers journaux automatiques*

À l'instar de la plupart des appareils numériques, lorsqu'ils sont en fonctionnement, les UAV génèrent régulièrement des données numériques qui sont conservées et les aident à continuer à fonctionner comme prévu. Si ces données ne sont pas destinées à être consultées par les utilisateurs – dont la plupart ignorent en fait l'existence –, certains UAV créent et stockent des fichiers journaux contenant des informations comme les détails des missions, l'heure et la date des opérations, ainsi que les points de passage lors du vol. Ces données incluent généralement des coordonnées GPS, la vitesse du moteur, l'altitude et des informations directionnelles.

## **2.7.2 Accès à différents supports de stockage des données**

La diversité des appareils/sources d'éléments de preuve offre aux enquêteurs de nombreuses possibilités car elle leur permet, si nécessaire, d'accéder à des données nombreuses et détaillées concernant le propriétaire d'un appareil ou l'utilisation qui en est faite, à partir des différents supports de stockage. Notre étude a montré que le mode de stockage et de conservation des données est foncièrement différent selon le fabricant et les caractéristiques techniques des drones. On peut ainsi avoir accès à de très faibles quantités de données numériques – voire aucune – sur les drones récréatifs bas de gamme, ou au contraire à une multitude de données complexes sur les modèles commerciaux et sur mesure.

Outre leurs quantités, l'emplacement des données peut aussi être très différent selon les caractéristiques techniques des drones et la configuration choisie par l'utilisateur. Il est donc crucial, lorsqu'il s'agit d'accéder aux données d'un UAV, d'adopter le principe du profilage, en déterminant le profil technique général et les compétences numériques de l'utilisateur, les caractéristiques techniques du drone, ses charges utiles éventuelles et la configuration du contrôleur de vol. Une fois ces éléments recueillis, une évaluation éclairée peut être établie concernant l'emplacement où peuvent se trouver les informations pertinentes pour l'enquête.

Ces informations peuvent se trouver à différents endroits, dont les suivants :

### *a) Dispositifs de stockage intégrés*

Sur certains drones, les informations sont stockées et conservées dans la mémoire et les processeurs intégrés au châssis ou au contrôleur de vol de l'appareil. Selon les caractéristiques techniques de l'UAV et les ports dont il est équipé, l'extraction des données peut se faire soit à l'aide d'une méthode relativement simple (comme le « Plug and play », c'est-à-dire en connectant un autre support de stockage), soit avec des techniques plus avancées et destructrices comme le retrait de la puce mémoire.

### *b) Supports de stockage amovibles*

Compte tenu de la taille des fichiers qui y sont stockés, la plupart des drones destinés à prendre des photos ou réaliser des vidéos haute résolution peuvent héberger des supports de stockage amovibles. Des cartes mémoire Micro SD d'une capacité pouvant aller jusqu'à 2 To sont aujourd'hui disponibles ; ce sont les supports qui offrent la plus grande capacité de stockage au meilleur prix, tout en occupant peu d'espace, et donc les plus répandus sur les UAV. Il faut également savoir que si le principal usage d'un support de stockage externe peut être d'y enregistrer des fichiers multimédias, ce périphérique peut aussi contenir d'autres types de fichiers.

### c) Périphériques et applications mobiles

Il est possible, sur de nombreux UAV, de contrôler partiellement ou totalement l'appareil ou sa charge utile par l'intermédiaire d'une connexion à Internet ou d'une application native installée sur un smartphone. Cette source potentielle de données ne doit pas être sous-estimée. Il convient, lors du profilage numérique, d'examiner quelles applications sont installées sur le périphérique mobile fixé au drone et quelles informations elles peuvent fournir pour les besoins de l'enquête.

### d) Télécommande

La plupart des drones s'accompagnent d'une télécommande spécifique. Celle-ci peut contenir des données résiduelles susceptibles d'aider à reconnaître le drone qui lui est associé ainsi que les éventuels smartphones ou tablettes utilisés pour visualiser les images prises par l'appareil.

### e) Postes de contrôle au sol

Les systèmes de contrôle ayant une liaison au sol pour la planification de l'itinéraire du vol, le mode immersion ou le suivi visuel peuvent enregistrer leurs données de fonctionnement ou les prises de vues sur un périphérique local tel qu'un disque dur d'ordinateur. L'accès à ces données instructives peut se faire en utilisant un logiciel intégré qui visualise les données là où elles se trouvent ou, en son absence, en procédant à l'examen sommaire de l'ordinateur ou en employant des techniques classiques de criminalistique numérique.

### f) Plateformes infonuagiques

La banalisation incessante et l'accessibilité croissante des solutions de stockage infonuagiques impliquent qu'on ne saurait les sous-estimer en tant que sources potentielles de données. Les données peuvent être stockées volontairement sur le nuage par l'utilisateur afin de réduire les besoins de stockage locaux, ou être générées par une plateforme infonuagique qui les conserve pour le compte de ses clients.

### g) Données par paquets provenant des réseaux

Les contrôleurs sans fil envoient souvent des commandes au drone et communiquent avec lui via les réseaux non filaires. Ces données par paquets provenant des réseaux représentent une source supplémentaire d'éléments de preuve numériques. Le déploiement du réseau Internet 5G devrait entraîner une hausse de l'utilisation des réseaux cellulaires pour contrôler les drones, ce qui fera de ces réseaux une source potentielle de précieux éléments de preuve.

## 2.7.3 Ce qu'il faut savoir sur les données lors des enquêtes concernant des drones

Compte tenu de la nature des données qu'ils renferment et du fait que les drones utilisent aussi d'autres supports de stockage, certaines choses sont à savoir.

Ce qu'il faut savoir sur les données lors des enquêtes concernant des drones
• Les données peuvent être disséminées sur plusieurs supports physiques, parfois dans différents pays.
• Les données peuvent être transférées d'un pays à un autre sans effort et en l'espace de quelques secondes.
• Les données sont très fragiles : elles peuvent être facilement modifiées, remplacées, altérées ou supprimées, et ce à l'aide d'une seule touche de clavier.
• Les données peuvent être copiées sans subir d'altération.
• Contrairement à ce qui se passe dans d'autres domaines de la police scientifique, les éléments de preuve électroniques ont une courte durée de vie et deviennent ensuite inutilisables. Au bout de cinq ans, le périphérique sur lequel ils se trouvent peut ne plus se mettre en marche ni fonctionner correctement.

Tableau 1 - Ce qu'il faut savoir sur les données lors des enquêtes concernant des drones

La conclusion de ces remarques est que les éléments de preuve relatifs aux drones doivent être traités et manipulés avec soin.

Des informations complémentaires et des consignes avancées concernant la façon de repérer, d'acquérir, d'analyser et d'interpréter les données provenant des drones seront fournies prochainement dans un module INTERPOL de perfectionnement sur l'analyse criminalistique des drones, qui est en cours d'élaboration.

## 2.8 Infractions pouvant être commises avec un drone

Dans le contexte de la nouvelle menace que représentent les drones et du risque qu'ils font courir aux personnes et aux biens lorsque leur utilisation n'est pas conforme aux réglementations et aux procédures de délivrance d'un permis, un certain nombre d'infractions ont récemment été commises. Ces infractions varient selon les pays, raison pour laquelle il est conseillé aux premiers intervenants d'avoir au moins une connaissance de base de la législation applicable aux drones.

Voici quelques exemples d'infractions liées aux drones :

- Absence de maintien d'un contact visuel direct avec le drone.
- Dépassement de l'altitude de vol autorisée localement (au Royaume-Uni et aux États-Unis, par exemple, l'altitude maximale autorisée est de 400 pieds ou 122 mètres).
- Pénétration de l'espace aérien sans autorisation.
- Pénétration dans des espaces aériens réglementés tels qu'un aéroport, une base militaire ou une infrastructure critique (une centrale nucléaire, par exemple).
- Vol non sécurisé (par exemple dans de mauvaises conditions météorologiques).
- Utilisation non autorisée d'un aéronef de surveillance (par exemple d'un UAV pour de la surveillance/violation de la vie privée).
- Mise en danger d'un aéronef civil (en volant trop haut, dans l'enceinte d'un aéroport ou dans un espace aérien réglementé).

Par ailleurs, dans certains pays, il est interdit pour un drone de survoler des personnes (en particulier des foules), de transporter une charge alors que l'appareil en question n'a pas été conçu pour cela, et de larguer des objets.

Les aspects à examiner en cas d'infraction liée à un drone sont les suivants :

- Quels sont les faits à établir ?
- Où a eu lieu l'infraction ?
- Quel jour et à quelle heure ?
- Le pilote et d'autres suspects ont-ils été identifiés et arrêtés ?
- Quel était le but du vol du drone ?
- Une cible était-elle visée ? Si oui, quelle était cette cible et quel était l'objectif de l'exploitant du drone ?

Un autre aspect important à prendre en compte est que, même si c'est le drone qui représente la menace, la cible de l'enquête doit être le pilote et les autres suspects.

## 2.9 Vue d'ensemble de la législation sur les drones

Bien que les approches de la réglementation des drones soient très variables selon les pays, certains éléments sont sensiblement les mêmes. La plupart des pays accordent la priorité à la sécurité et exigent parfois l'enregistrement du drone ou du pilote, ou des deux. Même dans les pays où une législation sur les drones existe déjà, la loi ne cesse d'être révisée. Il peut y avoir une réglementation sur les drones ainsi que sur l'espace aérien dans lequel ils évoluent. La plupart des dispositions légales et réglementaires sont établies par l'autorité nationale de l'aviation civile. Certains pays ont totalement interdit ces engins. Dans ces pays, tout voyageur qui est porteur d'un drone peut se le faire confisquer par les douanes, et tout utilisateur surpris en train de le faire voler risque une amende ou une peine de prison.

Les pays ayant interdit les drones (liste datant d'août 2019) sont les suivants :

Algérie, Barbade, Brunéi, Côte d'Ivoire, Cuba, Iran, Iraq, Kirghizistan, Madagascar, Maroc, Nicaragua, Sénégal et Syrie.

Tout fonctionnaire chargé de l'application de la loi est tenu de connaître la législation applicable dans son pays. Une majorité de pays ont confié à leur autorité de l'aviation civile le soin d'élaborer la législation se rapportant aux drones.

L'absence de législation sur les drones ne signifie pas nécessairement qu'il soit possible de faire voler ces engins n'importe où et n'importe comment. Cela peut en fait vouloir dire que les autorités des pays concernés sont globalement opposées à l'utilisation de drones sur leur territoire, en particulier par les touristes. La même prudence est également de mise lors du passage en douane d'un drone. Lorsqu'un pays ne possède pas de loi spécifique sur les UAV, il arrive que les fonctionnaires des douanes les confisquent, mais ce n'est pas systématique. Dans les pays où il existe une législation sur les drones/UAS, c'est généralement l'administration nationale ou l'autorité de l'aviation civile qui l'établit et veille à son application.

En cas de doute concernant la législation sur les drones applicable dans tel ou tel pays, il est recommandé de prendre contact avec l'autorité nationale de l'aviation pour connaître les dispositions les plus récentes. De nombreux pays mettent aujourd'hui à disposition des applications mobiles (disponibles sur Google Play pour Android ou Apple App Store pour iPhone) permettant de consulter les réglementations locales applicables et de visualiser les cartes des zones où le vol de drones est autorisé.

## 2.10 Consignes pour un usage des drones en toute sécurité

Lorsque l'on utilise un drone dans un pays où il n'existe pas de législation connue sur le sujet, le minimum est de respecter les consignes ci-dessous (tirées du « Drone Advisory » de l'administration fédérale de l'aviation des États-Unis et du « Drone Code » de l'autorité de l'aviation civile du Royaume-Uni) :

<b>Consignes pour un usage des drones en toute sécurité</b>	
<b>1</b>	Conserver un contact visuel direct avec le drone.
<b>2</b>	Respecter les spécifications du fabricant en matière de conditions météorologiques.
<b>3</b>	Maintenir une distance de 45 mètres environ avec les personnes et les biens. Ne pas faire voler le drone en direction des gens.
<b>4</b>	Se maintenir à 150 mètres environ des foules et des zones bâties.
<b>5</b>	Ne pas dépasser une altitude de vol d'environ 60 mètres (Singapour)/120 mètres (États-Unis).
<b>6</b>	Faire voler l'engin de jour ou au crépuscule civil.
<b>7</b>	Ne pas dépasser une vitesse de 1,5 km/h.
<b>8</b>	Céder le passage aux aéronefs pilotés.
<b>9</b>	Ne pas propulser le drone depuis un véhicule en mouvement.
<b>10</b>	Ne pas s'approcher à moins de 5 km d'un aéroport ou d'une infrastructure critique comme une centrale nucléaire, une base militaire ou une zone réglementée (telle que définie par le pays).

*Tableau 2 - Consignes pour un usage des drones en toute sécurité*

En cas de doute, demander conseil à l'autorité de l'aviation civile.

D'autres recommandations d'usage sont fournies sur les figures 11 et 12.



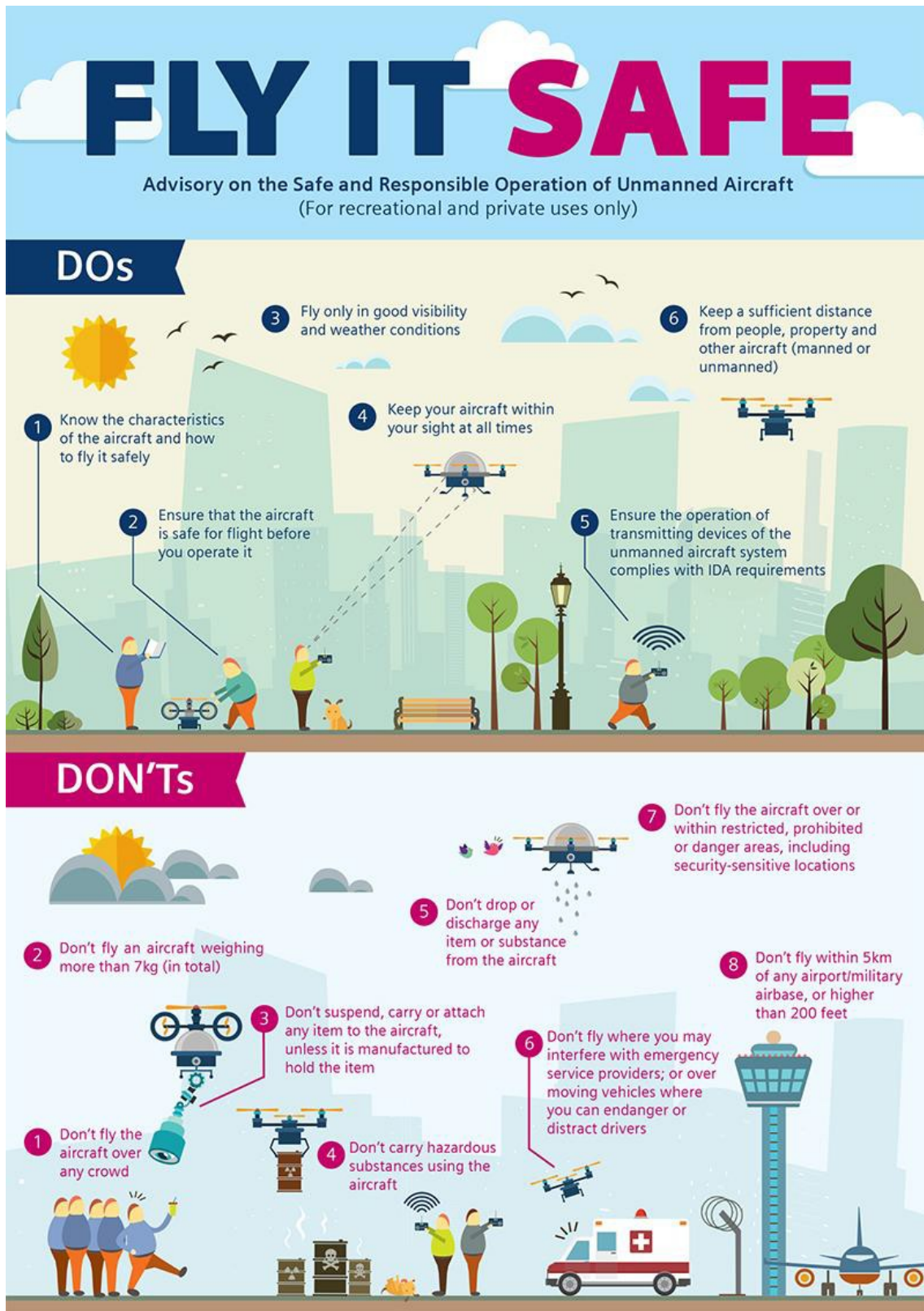


Figure 11 : Document infographique sur l'usage des drones en toute sécurité établi par l'autorité de l'aviation de Singapour

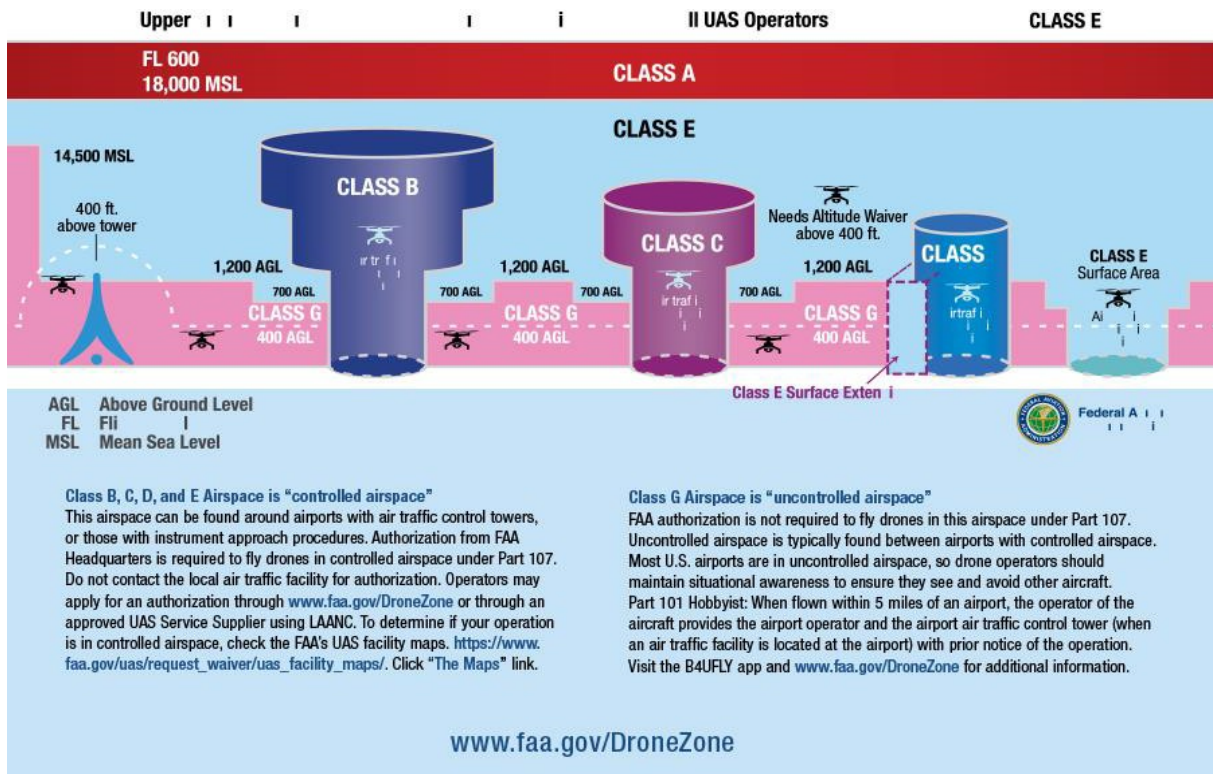


Figure 12 : Document infographique sur la classification des véhicules sans pilote établi par l'administration fédérale de l'aviation des États-Unis

### 2.11 Exemples de drones et équipements associés



Figure 13 : Télécommande de drone avec écran intégré

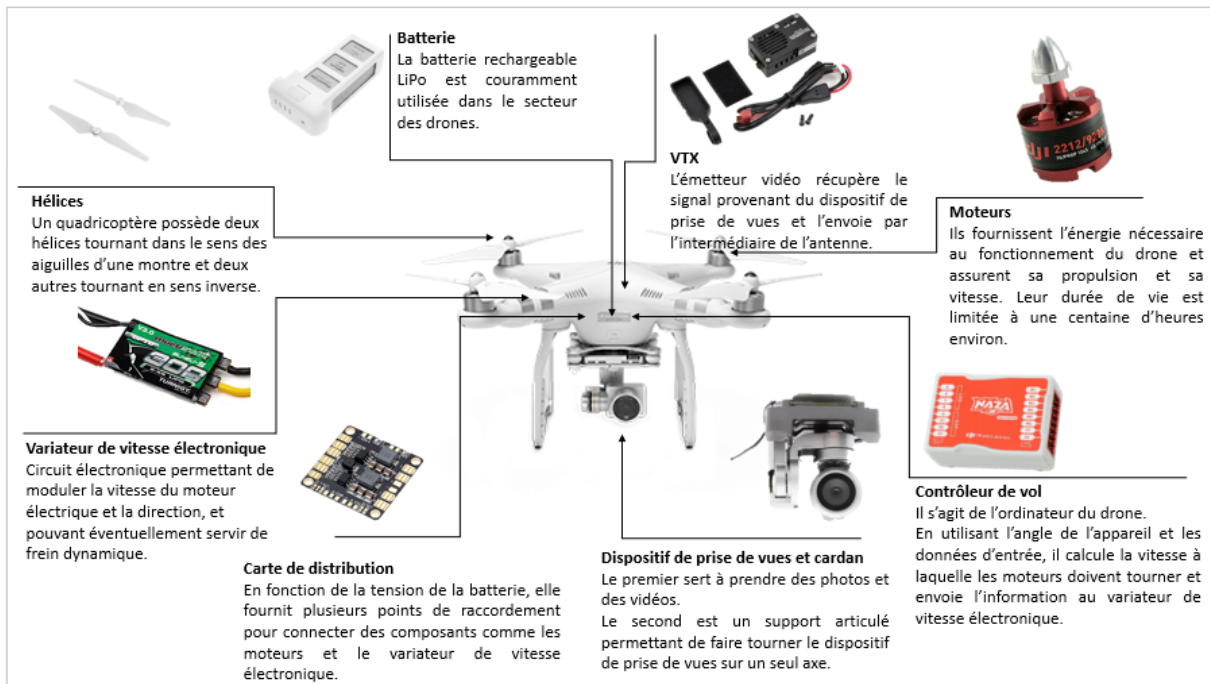


Figure 14 : Vue d'ensemble des composants d'un quadricoptère

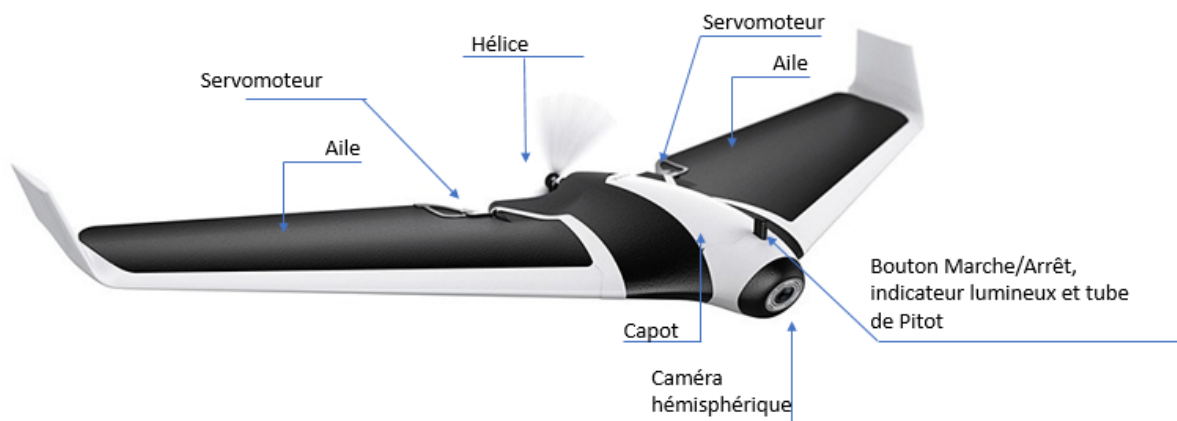


Figure 15 : Vue d'ensemble des composants d'un drone à voilure fixe



Figure 16 : Télécommande sans écran

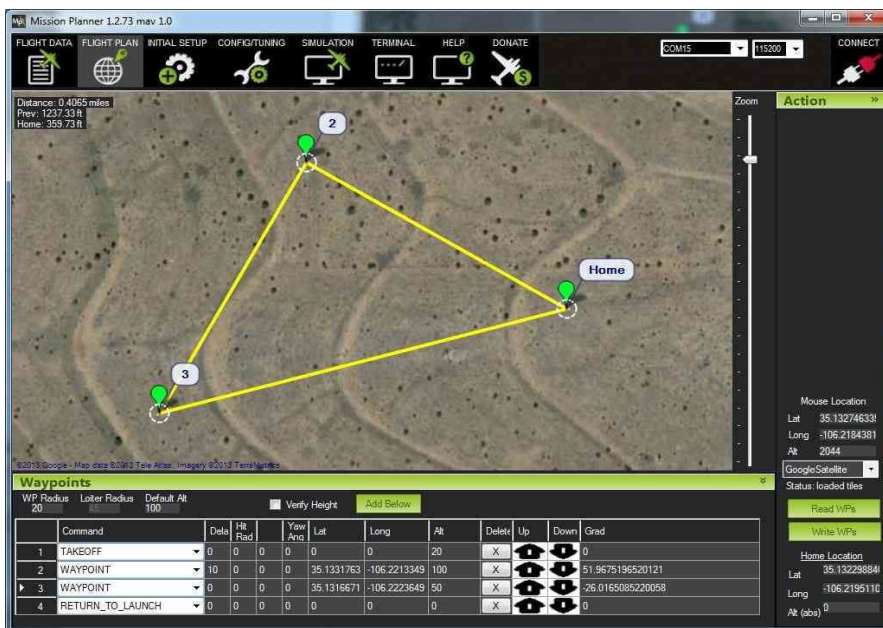


Figure 17 : Télécommande avec support pour smartphone





Figure 18 : Application mobile de contrôle



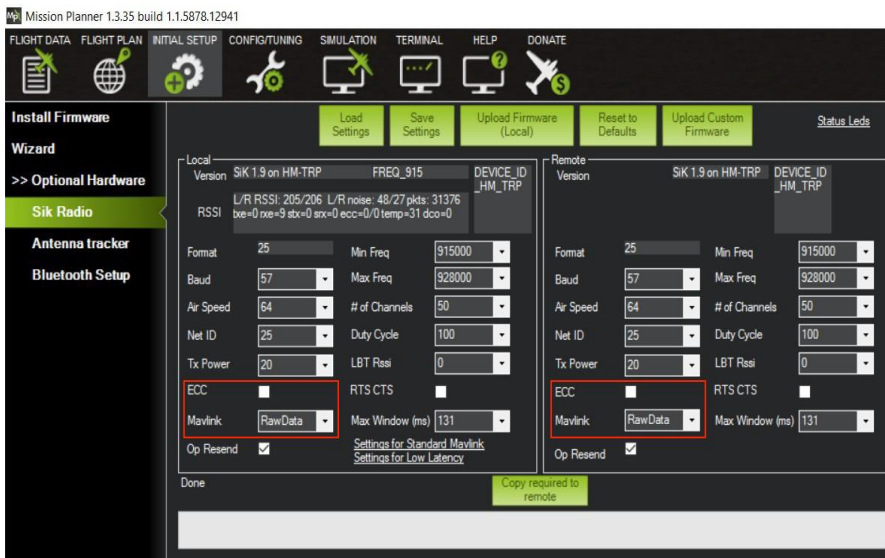


Figure 19 : Planificateur de mission

### 3. CONSIGNES A L'INTENTION DES PREMIERS INTERVENANTS

Ces consignes ont pour but de favoriser le maximum de pistes d'investigation possible, ainsi que de garantir la sécurité de l'enquêteur et du public.

Étapes de traitement d'une scène de crime	
1	Première intervention/Prise d'informations
2	Procédures de sécurité
3	Soins d'urgence
4	Sécurisation et contrôle des personnes présentes sur la scène
5	Délimitation de la scène : repérage, mise en place, protection et sécurisation
6	Transfert de la gestion de la scène de crime et compte rendu à l'enquêteur chargé de l'affaire
7	Consignation par écrit des actions et des observations
8	Établissement d'un poste de commandement (système de commande d'incident) et envoi de messages
9	Gestion des témoins
10	Évaluation de la scène
11	Inspection de la scène et premiers relevés
12	Prise de notes et tenue d'un registre

Tableau 3 - Étapes de traitement d'une scène de crime

#### 3.1 Première intervention/Prise d'informations

**Principe :** L'un des aspects les plus importants de la sécurisation de la scène de crime est de faire en sorte que les éléments de preuve matériels subissent le moins de contamination et de perturbation possible. La première intervention en cas d'incident doit être rapide et méthodique.

**Pratique :** Dès leur arrivée, les policiers primo-intervenants évaluent la scène et traitent l'incident comme s'il s'agissait d'une scène de crime. Ils y pénètrent rapidement, quoique avec précaution, en observant attentivement les éventuels personnes, véhicules, faits, éléments de preuve et conditions environnantes.



**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Noter ou enregistrer les informations émanant du centre d'appels (adresse/lieu, heure, date, type d'appel et parties prenantes).
<b>b</b>	Faire attention aux personnes ou véhicules quittant éventuellement la scène de crime.
<b>c</b>	Approcher la scène avec précaution, balayer du regard toute la zone afin d'évaluer l'ensemble de la scène et relever d'éventuelles scènes de crime annexes.
<b>d</b>	Être attentifs aux personnes et véhicules se trouvant éventuellement à proximité et pouvant avoir un lien avec l'infraction. Effectuer de premiers constats (visuels, auditifs et olfactifs) pour évaluer la scène en veillant au préalable à se protéger.
<b>e</b>	Rester alertes et attentifs. Procéder, sauf preuve du contraire, comme si l'infraction était toujours en cours.
<b>f</b>	Traiter la zone comme une scène de crime jusqu'à ce que l'analyse ait apporté la preuve du contraire.
<b>g</b>	Envoyer sur zone d'autres unités d'intervention en veillant à ce que leur sécurité soit assurée.

Tableau 4 - Procédure de la première intervention/prise d'informations

**En bref :** Il est important que les policiers primo-intervenants fassent très attention lorsqu'ils approchent une scène de crime, y pénètrent et en sortent. Ils doivent en outre assurer la sécurité des fonctionnaires chargés de l'application de la loi et du public situé dans la zone ou à proximité.

**3.2 Procédures de sécurité**

**Principe :** La priorité numéro un des premiers intervenants est d'assurer la sécurité et le bien-être physique des policiers et autres personnes se trouvant sur la scène de crime et autour.

**Pratique :** Les policiers primo-intervenants arrivant sur la scène de crime doivent repérer et gérer les éventuelles personnes ou situations dangereuses.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	S'assurer qu'il n'existe pas de menace immédiate pour les autres intervenants ; vérifier par la vue, l'ouïe et l'odorat qu'il n'y a pas de danger pour le personnel (par exemple, des matières dangereuses comme des charges utiles contenant un engin explosif artisanal ou des substances présentant un risque biologique). Si la présence d'une charge utile, d'armes biologiques ou de menaces chimiques ou radiologiques est constatée, il convient de contacter le personnel/service compétent avant que quiconque ne pénètre sur la scène.
<b>b</b>	Approcher la scène de manière à réduire les risques de danger pour eux-mêmes, tout en veillant à la sécurité maximale des victimes, témoins et autres personnes présentes.
<b>c</b>	Surveiller la présence éventuelle d'individus dangereux sur la scène et contrôler la situation.
<b>d</b>	Informers les supérieurs hiérarchiques et demander de l'aide/des secours.

Tableau 5 - Procédures de sécurité

**En bref :** La gestion des menaces physiques garantira la sécurité des policiers et autres personnes présentes.

### 3.3 Soins d'urgence

**Principe :** Une fois que les éventuelles situations ou personnes dangereuses ont été maîtrisées, la tâche des premiers intervenants est de s'assurer que des soins médicaux sont prodigués aux blessés tout en évitant au maximum la contamination de la scène.

**Pratique :** Les policiers primo-intervenants s'assurent que des soins médicaux sont prodigués tout en évitant au maximum la contamination de la scène.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Évaluer les signes vitaux et les besoins médicaux des victimes et leur prêter immédiatement attention.
<b>b</b>	Appeler le personnel médical.
<b>c</b>	Guider le personnel médical vers les victimes afin de minimiser la contamination/l'altération de la scène de crime.
<b>d</b>	Signaler au personnel médical les éléments de preuve matériels éventuels et leur demander d'avoir le moins de contact physique avec eux (par exemple : s'assurer que le personnel médical préserve intacts les vêtements et effets personnels sans les couper autour des perforations dues à des balles, des déchirures faites à l'aide d'un couteau, etc.). Consigner par écrit tout déplacement des personnes ou des objets effectué par le personnel médical.
<b>e</b>	Demander au personnel médical de ne pas nettoyer la scène, et d'éviter de retirer ou d'altérer les objets qui s'y trouvent.
<b>f</b>	Si le personnel médical est arrivé en premier, se procurer les noms, unités et numéros de téléphone des membres qui le composent, ainsi que le nom et l'adresse de l'établissement médical où vont être transférées les victimes.
<b>g</b>	Si une victime risque de décéder, tenter d'obtenir une « déclaration de mourant ». Dans certains cas, les empreintes digitales et les traces de chaussures du personnel médical doivent être prélevées afin qu'elles puissent être éliminées.
<b>h</b>	Noter par écrit les déclarations/commentaires pouvant avoir été formulés par les victimes, les suspects ou les témoins sur la scène.
<b>i</b>	Si une victime ou un suspect est transféré dans un établissement médical, les faire accompagner par un fonctionnaire chargé de l'application de la loi pour noter leurs éventuels commentaires et préserver les éléments de preuve. (Si aucun fonctionnaire n'est disponible, rester sur la scène de crime et demander au personnel médical de préserver les éléments de preuve et de noter les éventuels commentaires de la victime ou du suspect.)
<b>j</b>	Protéger les éléments de preuve, comme par exemple une charge utile. Dès qu'un élément de preuve est saisi, suivre la procédure de conservation applicable.

Tableau 6 - Procédure des soins d'urgence

**En bref :** Le fait d'aider et de guider le personnel médical, ainsi que de lui donner des instructions lors des soins prodigués aux blessés et de leur transfert hors de la scène, permet de réduire les risques de contamination et de destruction de preuves.

### 3.4 Sécurisation et contrôle des personnes et des éventuels éléments de preuve sur la scène

**Principe :** Contrôler, identifier et faire sortir les personnes présentes sur la scène de crime, ainsi que limiter le nombre de celles qui y pénètrent, est une tâche importante des policiers primo-intervenants pour protéger la scène.

**Pratique :** Les policiers primo-intervenants identifient les personnes présentes et limitent leurs mouvements.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Contrôler toutes les personnes présentes sur la scène : les empêcher d'altérer/de détruire des éléments de preuve matériels en limitant leurs mouvements et leur activité, ainsi qu'en assurant et maintenant la sécurité sur la scène.
<b>b</b>	Identifier toutes les personnes présentes sur la scène, telles que : <ul style="list-style-type: none"> <li>• Suspects : les sécuriser et les éloigner ;</li> <li>• Témoins : les sécuriser et les éloigner ;</li> <li>• Passants : déterminer s'ils ont assisté aux faits. Si oui, les traiter comme des témoins ; sinon, leur demander de quitter la scène.</li> <li>• Victimes/membres de la famille/amis : contrôler leur identité tout en faisant preuve de compassion.</li> <li>• Fonctionnaires des services chargés de l'application de la loi, personnel médical et personnel d'autres services d'assistance : les identifier.</li> </ul>
<b>c</b>	Interdire l'accès à toute personne non autorisée et non nécessaire (par exemple, des fonctionnaires chargés de l'application de la loi ne travaillant pas sur cette affaire, des responsables politiques ou les médias).

Tableau 7 - Procédure de sécurisation et de contrôle des personnes présentes sur la scène

**En bref :** Contrôler les mouvements des personnes présentes et limiter le nombre de celles qui y pénètrent sont des tâches essentielles pour préserver l'intégrité de la scène, sauvegarder les éléments de preuve et limiter au maximum la contamination.

### 3.5 Transfert de la gestion de la scène de crime et compte rendu à l'enquêteur chargé de l'affaire

**Principe :** Rendre compte de la situation à l'enquêteur chargé de l'affaire aide à gérer la scène de crime, à établir les responsabilités ultérieures de l'enquête, et à gérer les ressources.

**Pratique :** Les policiers primo-intervenants fournissent à l'enquêteur chargé de l'affaire un compte rendu détaillé de la scène de crime.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Fournir un compte rendu à l'enquêteur chargé de l'affaire.
<b>b</b>	Aider à la gestion de la scène de crime.
<b>c</b>	Transférer la responsabilité de l'enregistrement des entrées/sorties.
<b>d</b>	Rester sur la scène jusqu'à la relève des fonctions.

Tableau 8 - Procédure du transfert de la gestion de la scène de crime et du compte rendu à l'enquêteur chargé de l'affaire

**En bref :** Le compte rendu de la scène est la seule possibilité pour le fonctionnaire prenant en charge la suite des opérations de prendre connaissance de la situation avant d'ouvrir une enquête.

### 3.6 Consignation par écrit des actions et des observations

**Principe :** Tout ce qui a lieu et tout ce qui est observé sur la scène de crime doit être consigné par écrit aussitôt après les faits afin de garder une trace des informations.

**Pratique :** Les policiers primo-intervenants inscrivent ces informations dans un registre.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Noter ce qui est observé sur la scène de crime, notamment l'emplacement des personnes et des objets, ainsi que l'aspect général et l'ambiance de la scène à l'arrivée sur les lieux.
<b>a</b>	Noter les conditions ambiantes à l'arrivée sur les lieux (par exemple : lumières allumées/éteintes ; volets remontés/abaissés, ouverts/fermés ; fenêtres et portes ouvertes/fermées ; odeurs ; glace, liquides ; meubles ; météo ; température ; objets personnels).
<b>c</b>	Noter les informations personnelles fournies par les témoins, les victimes et les suspects, ainsi que toute déclaration ou tout commentaire qu'ils aient pu faire.
<b>d</b>	Noter les actions effectuées par les témoins, les victimes et les suspects, ainsi que toute autre personne.

Tableau 9 - Procédure de consignation par écrit des actions et des observations

**En bref :** Les policiers primo-intervenants doivent produire des informations claires, concises et détaillées sur les actions et ce qu'ils ont observé. Ces informations sont vitales pour l'enquête et la procédure judiciaire ultérieures.

### 3.7 Établissement d'un poste de commandement (système de commande d'incident) et envoi de messages

**Principe :** La mise en place d'un lieu où les activités d'investigation sur la scène de crime peuvent être coordonnées, où les médias peuvent être conviés, et où l'équipe peut se réunir est extrêmement utile. Ce lieu central où l'enquête peut être menée et où l'on peut évaluer les ressources équivaut à un poste de commandement. Ce poste permet également de tenir informées de l'enquête d'autres parties prenantes essentielles, et de les faire participer si nécessaire aux activités.

**Pratique :** L'enquêteur chargé de l'affaire choisit un lieu où les activités d'investigation sur la scène de crime peuvent être coordonnées, où les médias peuvent être conviés, et où l'équipe peut se réunir.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Mettre en place un poste de commandement temporaire à un endroit où les médias pourront prendre des photos sans compromettre la scène (ni les éléments de preuve).
<b>b</b>	Communiquer aux enquêteurs ou aux services appropriés (celui chargé des homicides, par exemple) les informations recueillies sur la scène de crime. Discuter des détails de la scène.
<b>c</b>	Transmettre au service des communications (centre d'appels) les numéros de téléphone du poste de commandement.
<b>d</b>	Lorsqu'un suspect s'est enfui de la scène, demander au service des communications (centre d'appels) d'informer les services situés à proximité et d'envoyer un message sur télécopieur aux niveaux régional et national. Ce message d'alerte doit inclure une description du suspect et des éventuels véhicules, ainsi que les coordonnées de la personne à contacter en cas de localisation de l'individu.
<b>e</b>	Informers si nécessaire le supérieur hiérarchique.
<b>f</b>	Établir un compte rendu de situation avec les premiers intervenants et les fonctionnaires chargés de l'application de la loi/enquêteurs.
<b>g</b>	Effectuer si nécessaire des assignations de missions, en les enregistrant dans un document prévu à cet effet.
<b>h</b>	Actualiser, sur ce document, les assignations de missions pendant toute la durée de l'enquête. Mettre ce document à la disposition du personnel travaillant sur l'affaire. Désigner une personne chargée d'enregistrer les éléments de preuve ainsi que les entrées/sorties (et également de mettre par écrit les faits et les horaires).
<b>i</b>	Déterminer le statut et l'adresse des victimes et des suspects.
<b>j</b>	Déterminer le statut des informations qui ont été diffusées concernant les victimes et les suspects. S'assurer que des alertes sont diffusées pour les suspects en fuite. Établir un programme de réunions de l'équipe chargée de l'enquête (y compris les policiers en uniforme) au cours desquelles un compte rendu de la situation sera donné, les assignations de missions seront actualisées et d'autres informations clés seront fournies.

Tableau 10 - Procédure d'établissement d'un poste de commandement (système de commande d'incident) et d'envoi de messages

**En bref :** L'établissement d'un poste de commandement est primordial pour la communication entre les premiers intervenants, le centre d'appels et d'autres personnes fournissant des informations à ceux qui interviennent sur la scène de crime.

### 3.8 Gestion des témoins

**Principe :** Il est crucial, pour résoudre une affaire criminelle, d'interroger rapidement les témoins.

**Pratique :** L'enquêteur chargé de l'affaire identifie les témoins de l'infraction et veille à leur protection. Il les interroge éventuellement sur place et leur réserve un traitement conforme aux réglementations applicables.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Interroger les témoins présents sur la scène séparément afin que leurs témoignages soient les plus utiles possible à l'enquête.
<b>b</b>	Transporter chaque témoin séparément des autres témoins ou suspects pour les conduire au commissariat.
<b>c</b>	Au commissariat, prendre la déposition écrite/audio de chaque témoin.
<b>d</b>	Lorsque c'est possible, le superviseur doit s'acquitter des tâches suivantes : <ul style="list-style-type: none"> <li>• Établir le statut et l'adresse de chaque victime et chaque suspect.</li> <li>• Établir le statut des informations qui ont été diffusées concernant chaque victime et chaque suspect. S'assurer que des alertes sont diffusées sans délai pour les suspects en fuite.</li> </ul>

Tableau 11 - Procédure de gestion des témoins

**En bref :** Il est important que chaque témoin soit interrogé séparément et sans délai pour obtenir des informations sur l'infraction.

### 3.9 Évaluation de la scène

**Principe :** L'évaluation de la scène par l'enquêteur chargé de l'affaire permet de déterminer le type d'incident sur lequel doit porter l'enquête et le niveau de cette enquête.

**Pratique :** L'enquêteur chargé de l'affaire établit les responsabilités, partage les informations préliminaires et conçoit le plan de l'enquête en tenant compte de la politique de son service ainsi que de la législation locale, fédérale et de l'État concerné.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Échanger avec les premiers intervenants concernant les actions et ce qu'ils ont observé.
<b>b</b>	Évaluer les aspects qui peuvent poser des problèmes de sécurité à toutes les personnes pénétrant sur la scène de crime (par exemple : éléments pathogènes du sang, dangers).
<b>c</b>	Évaluer les difficultés en matière de perquisition et de saisie afin de déterminer s'il est nécessaire d'obtenir une autorisation ou un mandat de perquisition.
<b>d</b>	Évaluer et établir une voie d'accès à/de retrait de la scène de crime qui pourra être utilisée par le personnel autorisé.
<b>e</b>	Déterminer les limites initiales de la scène de crime.
<b>f</b>	Déterminer le nombre/la taille des scènes et fixer un ordre de priorité.
<b>g</b>	Établir une zone de sécurité à proximité de la/des scène(s) pour en faire un espace de consultation et d'entreposage du matériel.
<b>h</b>	S'il existe plusieurs scènes de crime, établir et maintenir la communication avec le personnel intervenant sur chacune d'elles.
<b>i</b>	Établir une zone de sécurité pour y déposer temporairement les éléments de preuve en respectant la chaîne de conservation.

<b>j</b>	Déterminer les ressources supplémentaires nécessaires à l'enquête et en faire la demande (personnel/unités spécialisées, conseillers juridiques/procureurs, équipement).
<b>k</b>	Préserver en continu l'intégrité de la scène (par exemple : noter les entrées/sorties du personnel autorisé, empêcher l'accès à la scène à toute personne non autorisée).
<b>l</b>	S'assurer que les témoins de l'incident sont identifiés et séparés les uns des autres (leur demander, par exemple, une pièce d'identité en cours de validité).
<b>m</b>	S'assurer que la zone environnante a été examinée de façon approfondie et noter les résultats. Veiller à ce que des notes/photos préliminaires soient prises de la scène, des blessés et des véhicules.

Tableau 12 - Procédure d'évaluation de la scène

**En bref :** L'évaluation de la scène permet d'élaborer un plan de coordination des actions relatives aux éléments de preuve matériels (repérage, collecte et conservation) et de l'identification des témoins. Elle permet en outre l'échange d'informations entre les fonctionnaires chargés de l'application de la loi et la conception de stratégies concernant l'enquête.

### 3.10 Délimitation de la scène : repérage, mise en place, protection et sécurisation

**Principe :** Définir et protéger les limites de la scène permet de la protéger et de la sécuriser. Le nombre de scènes de crime et leur délimitation dépendent du lieu et du type d'infraction. Les limites sont fixées au-delà du cadre initial de la scène, en sachant qu'elles peuvent être revues à la baisse si nécessaire, mais plus difficilement étendues.

**Pratique :** Les policiers primo-intervenants procèdent à une première évaluation de l'étendue de la scène (ou des scènes) de crime puis définissent et protègent ses limites.

#### Procédure :

Tâches incombant aux policiers primo-intervenants	
<b>a</b>	Définir les limites de la/des scène(s), en commençant par le centre et en incluant : <ul style="list-style-type: none"> <li>• l'endroit où a eu lieu l'infraction ;</li> <li>• les points d'entrée et de sortie et passages éventuels des suspects et des témoins ;</li> <li>• les endroits où les victimes/des éléments de preuve risquent d'avoir été déplacés (faire attention aux traces et aux empreintes lors de l'évaluation de la scène).</li> </ul>
<b>b</b>	Sécuriser la scène. Installer des barrières physiques (par exemple des cordes, cônes, rubans de sécurité, véhicules, personnes ou matériel divers) ou utiliser les séparations existantes (comme des portes, murs, passerelles).
<b>c</b>	Une fois que les limites ont été établies, noter toutes les entrées et sorties.
<b>d</b>	Protéger la scène. Contrôler le flux des personnes et des animaux qui entrent et sortent, afin de préserver l'intégrité de la scène.
<b>e</b>	Prendre des mesures pour préserver/protéger les éléments de preuve qui peuvent être détruits ou dégradés, par exemple par les éléments météorologiques (pluie, vent, neige), des marques de pas, des traces de pneus et des systèmes d'arrosage.
<b>f</b>	Noter l'emplacement initial de la victime ou de tout objet en train d'être déplacé.
<b>g</b>	Évaluer les difficultés en matière de perquisition et de saisie afin de déterminer s'il est nécessaire d'obtenir une autorisation ou un mandat de perquisition.

Tableau 13 - Délimitation de la scène : repérage, mise en place, protection et sécurisation



**Note :** Il est INTERDIT aux personnes de fumer, d'utiliser le téléphone ou les toilettes, de manger ou de boire, de retirer quelque objet que ce soit de la scène y compris des armes (sauf si cela est nécessaire pour la sécurité et le bien-être des personnes présentes), de régler la température ou d'ouvrir les portes ou les fenêtres (afin de conserver la scène telle quelle), de toucher quoi que ce soit inutilement (noter et préciser tous les déplacements d'objets) ou de replacer des objets ayant été bougés au sein des limites de la scène. Interdire également aux suspects d'utiliser les toilettes ou de modifier leur apparence (notamment en se peignant les cheveux ou en se lavant les mains).

**En bref :** La délimitation de la scène de crime est essentielle pour garantir l'intégrité des éléments de preuve matériels.

### 3.11 Inspection de la scène et premiers relevés

**Principe :** L'inspection de la scène permet d'en avoir une vue d'ensemble, de repérer ce qui peut en menacer l'intégrité et d'assurer la protection des éléments de preuve matériels. Les relevés écrits et photographiques sont enregistrés de façon permanente. L'inspection ne doit avoir lieu que si les éléments de preuve seront maintenus intacts. Il peut être nécessaire de procéder immédiatement, avant l'inspection, au relevé et à la collecte des éléments de preuve.

**Pratique :** L'enquêteur chargé de l'affaire procède à l'inspection de la scène, en présence des personnes chargées de la gestion de la scène.

**Procédure :**

Tâches incombant aux policiers primo-intervenants	
a	Éviter la contamination de la scène en empruntant la voie d'accès préétablie.
b	Déterminer si des équipements de protection personnelle doivent être utilisés.
c	Procéder à la description préliminaire de la scène telle qu'elle se présente (par exemple avec des notes et des croquis).
d	Repérer et protéger les éléments de preuve fragiles et périssables (prendre en compte les conditions climatiques, la présence d'une foule ou d'un environnement hostile). Faire en sorte que tous les éléments de preuve susceptibles d'être compromis soient immédiatement consignés, photographiés et recueillis.
e	Lors de la première inspection de la scène, noter les conditions existantes. Enregistrer ce qui est observé, notamment les éléments suivants : <ul style="list-style-type: none"> <li>• Équipements extérieurs (lampadaire, panneau de signalisation, banc, etc.).</li> <li>• Points d'entrée et de sortie des bâtiments situés à proximité et environnement local.</li> <li>• Lieu de l'accident : des dégâts ont-ils été causés aux bâtiments ou à l'environnement proches ?</li> <li>• Éclairage public : allumé ou éteint ? Dans le premier cas, quelles lampes sont éclairées ?</li> <li>• Conditions météorologiques : heure de la journée, météo locale, vitesse du vent, etc.</li> <li>• Conditions au sol.</li> <li>• Luminosité extérieure.</li> <li>• Odeurs : fumée de cigarette, gaz, poudre, parfum, etc.</li> <li>• Description de l'auteur de l'infraction (s'il est présent).</li> <li>• Description des individus liés à l'infraction qui sont présents.</li> <li>• Description du personnel des services médicaux d'urgence ou des équipes de recherche et sauvetage qui sont présents.</li> <li>• Armes.</li> <li>• Mobilier et son emplacement par rapport à la victime et à l'ensemble de la scène.</li> <li>• Théorie générale sur l'infraction.</li> </ul>

Tableau 14 - Procédure d'inspection de la scène et de réalisation des premiers relevés

**En bref :** L'inspection de la scène permet à l'enquêteur chargé de l'affaire d'avoir une vue d'ensemble. Elle offre une première possibilité de repérer les éléments de preuve fragiles et utiles, ainsi que de définir les étapes initiales de l'enquête grâce à l'examen systématique de la scène et aux relevés qui sont effectués. Les relevés écrits et photographiques permettent de conserver une trace permanente de la scène telle qu'elle a été observée initialement et constituent des pièces importantes.

### 3.12 Prise de notes et tenue d'un registre

**Principe :** La prise de notes et la tenue d'un registre permettent de conserver une trace permanente des activités ayant lieu sur la scène de crime.

**Pratique :** Toutes les personnes participant à l'examen de la scène de crime prennent des notes et inscrivent leurs activités sur un registre.

**Procédure :** Un registre détaillé est établi sur les entrées/sorties. Il permet de noter les personnes qui entrent et sortent sur/de la scène de crime au cours de l'enquête. Les personnes qui étaient présentes avant le début de la procédure y sont également notées.

#### Tâches incombant aux policiers primo-intervenants

<b>a</b>	Le fonctionnaire qui tient le registre est désigné par le superviseur et s'acquitte de cette tâche à temps plein. Il veille à ce que le registre soit complété le plus précisément possible et s'assure que toute personne pénétrant sur la scène a un rôle défini à y jouer.
<b>b</b>	Le registre est placé à un endroit très visible, de sorte que chaque personne puisse le compléter en entrant et en sortant. Il doit contenir les informations suivantes : <ul style="list-style-type: none"> <li>• Lieu de la scène de crime ;</li> <li>• Noms des témoins ;</li> <li>• Noms des victimes ;</li> <li>• Noms des personnes placées en garde à vue ;</li> <li>• Noms des premiers intervenants et heures approximatives d'arrivée ;</li> <li>• Nom du superviseur et heure approximative d'arrivée (une heure approximative doit être indiquée si l'intéressé est arrivé avant que le registre ne soit mis en place).</li> </ul>
<b>c</b>	Indiquer, pour chaque personne présente sur la scène, les informations ci-dessous. Si un registre ou formulaire non officiel est utilisé, laisser de l'espace pour les inscrire : <ul style="list-style-type: none"> <li>• Date d'arrivée ;</li> <li>• Heure d'arrivée ;</li> <li>• Nom ;</li> <li>• Numéros d'identification et de l'unité ;</li> <li>• Organisation (si autre que le service chargé de l'enquête) ;</li> <li>• Raison de la présence sur la scène (il convient d'inscrire sur le registre les heures d'arrivée et de départ de toutes les personnes présentes, y compris l'officier de police judiciaire, le spécialiste de criminalistique numérique ou toute autre personne jouant un rôle essentiel).</li> <li>• Informations sur les personnes présentes et raisons de leur présence sur la scène de crime ; numéro de l'incident ; noms des premiers intervenants, de l'officier responsable du registre et du superviseur, numéros de leurs badges et de leurs unités ; lieu de la scène de crime ; noms des victimes, suspects, témoins, etc.</li> </ul>

### Tâches incombant aux policiers primo-intervenants

- Avant d'autoriser l'accès de la scène à des visiteurs, inscrire sur le registre des entrées/sorties les informations logistiques (heure, lieu de la scène de crime, noms des victimes, suspects, témoins, etc.).
- S'assurer que chaque fois qu'une personne quitte la scène, son heure de départ est enregistrée avant qu'elle parte.
- Si quelqu'un quitte la scène sans en informer l'officier responsable du registre, ce dernier peut inscrire l'heure de départ estimée ainsi qu'une note indiquant la raison pour laquelle il s'agit d'une estimation.
- Placer le registre dans un lieu sûr, en respectant les réglementations applicables.

Tableau 15 - Procédure de prise de notes et de tenue d'un registre

**En bref :** La prise de notes et la tenue d'un registre des entrées/sorties ont pour but d'enregistrer les personnes présentes sur la scène de crime pour les besoins de l'enquête et de la procédure judiciaire.

### 3.13 Saisie d'un drone

Les consignes suivantes visent à faire en sorte que les saisies de drones aient lieu pour la plupart selon les bonnes pratiques reconnues.

Avant toute intervention, il est conseillé si possible de déterminer la marque et le modèle du drone, puis d'effectuer une recherche approfondie afin de déterminer les capacités de l'appareil, ainsi que l'emplacement de ses dispositifs de stockage de données et des possibilités qu'il offre de recueillir des éléments de preuve et des renseignements numériques. Avant toute interaction avec le drone ou son utilisateur, réfléchir à la manière de recueillir les meilleures preuves possibles de l'infraction dont vous avez été témoin ou pour laquelle vous avez été appelé à intervenir.

Après quoi, si vous considérez qu'il est utile de saisir l'appareil et si vous souhaitez le faire, veillez à suivre la procédure ci-dessous :

#### Processus de saisie d'un drone

- 1** Avant toute interaction physique avec le drone et la télécommande, réfléchir aux possibilités de recueillir des éléments de preuve humides (ADN et empreintes digitales). Avant d'envisager les possibilités de saisie et d'emballage des appareils, veiller à les manipuler de façon à préserver les éventuels éléments de preuve. Par exemple, porter des gants, faire attention aux zones pouvant recéler des éléments de preuve humides (boutons de mise en marche, ports de connexion des câbles, levier de commande, etc.), et procéder à l'emballage avec précaution.
- 2** Examiner rapidement à proximité s'il y a des appareils avec lesquels le drone pourrait être connecté ou associé. La plupart des drones ont une faible portée et les systèmes de contrôle/antennes se trouvent généralement pas très loin. Essayer de localiser le pilote.
- 3** Si possible, approcher le drone par derrière et éteindre toute source de lumière afin d'éviter d'être repéré par le pilote. Déterminer si l'appareil est allumé (il y a généralement des lumières ou du bruit sur l'unité) ou éteint. Évaluer son degré de puissance et s'il a été mis en route depuis votre arrivée. Si le drone est allumé, observer et enregistrer les informations affichées sur ses écrans. Empêcher le drone de s'envoler (sans l'abîmer, par exemple en le recouvrant d'un vêtement ou d'un filet, ou en le renversant) jusqu'à être en capacité de l'éteindre en toute sécurité sans compromettre les données qu'il contient.

Processus de saisie d'un drone	
4	Enregistrer les principaux identifiants de l'UAV, notamment le fabricant, le modèle et le numéro de série. Ces identifiants peuvent figurer à différents endroits selon le modèle. Certains drones comportent un code QR qui, une fois lu, permet leur identification.
5	Si le drone est équipé d'une batterie amovible, la retirer de l'appareil. Si la batterie n'est pas amovible, éteindre le drone en appuyant une fois sur le bouton d'alimentation, puis une deuxième fois en maintenant le bouton enfoncé pendant deux secondes (sur les modèles DJI), ou en appuyant sur le bouton d'arrêt (selon le modèle). Enregistrer l'heure à laquelle chacune de ces tâches est effectuée. <b>ATTENTION</b> : Si la batterie présente des signes de dommage ou de fuite, ne pas la retirer ni la manipuler car elle pourrait exploser ou causer des blessures.
6	Prendre note de toute modification facilement repérable ayant été apportée au drone ou de la présence, sur l'appareil ou à proximité, d'un équipement annexe ou d'une charge utile.
7	Placer le drone et la télécommande séparément dans deux cages/sacoques de Faraday distinctes afin d'empêcher la pollution de l'air et l'effacement à distance des données. Placer les appareils auxquels le drone est connecté/associé dans des cages de Faraday distinctes, mais en indiquant qu'ils ont été trouvés à proximité. Les appareils ayant un lien avec le drone mais séparés de lui/trouvés à distance doivent être traités comme des pièces à conviction indépendantes, et emballés en conséquence.

Tableau 16 - Processus de saisie d'un drone

Il est très important que le drone et les équipements qui y sont associés soient récupérés avec le moins de perte de données possible, afin d'optimiser les chances de pouvoir accéder aux données historiques et identifier l'utilisateur. Afin d'aider les premiers intervenants, INTERPOL a créé un formulaire de « Compte rendu d'incident lié à un drone par les premiers intervenants » qui leur permet d'enregistrer et de documenter l'infraction et les événements connexes (voir l'annexe B).

Lorsque survient un incident lié à un drone, il est crucial de respecter les consignes suivantes. La première priorité est la sécurité des premiers intervenants, des services d'urgence et du public.

Dès leur arrivée, les premiers intervenants doivent évaluer la scène de crime et s'assurer que personne ne risque d'être blessé ou tué. Avant de s'approcher du drone, ils doivent déterminer pour quelle raison l'engin se trouve là.

- S'est-il écrasé ou a-t-il atterri de lui-même ?
- La cible visée est-elle identifiable ?
- Le pilote du drone peut-il être localisé ?
- Le drone comporte-t-il une charge utile ? Si oui, cette charge présente-t-elle un risque, par exemple un engin explosif artisanal ou un risque biologique ?

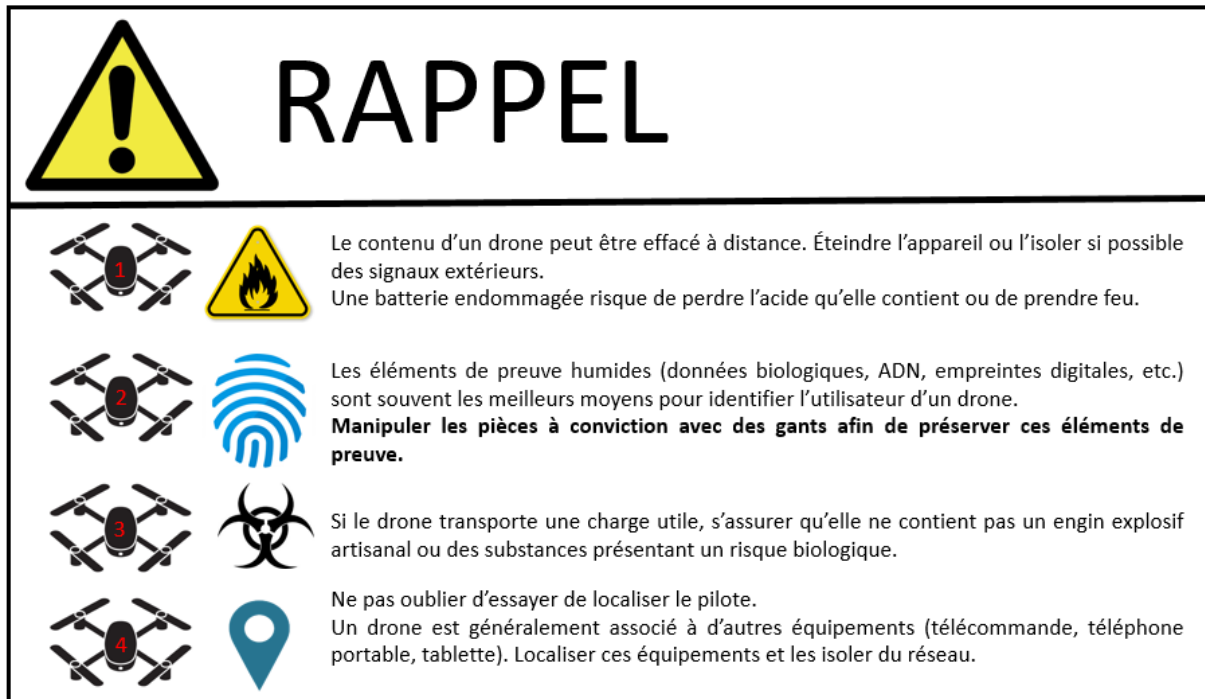


Figure 20 : Précautions à prendre avant de s'approcher d'un drone dans le contexte d'un incident

Une fois que la scène a été évaluée et qu'il est sûr qu'elle ne présente aucun risque pour eux-mêmes, le personnel des services d'urgence ou le public, les premiers intervenants peuvent envisager de s'approcher du drone.

Dans ce cas, il est préférable de s'approcher du drone par derrière, afin de ne pas être vu du pilote par le biais d'un écran.

Les principaux dangers proviennent des hélices du drone, si elles sont encore en mouvement. Lorsque l'engin est en marche, il peut soudainement tenter de décoller. Pour éviter cela, une possibilité est de le recouvrir avec un vêtement lourd ou une couverture, ou de le renverser afin qu'il ne puisse pas décoller.

La priorité est de sécuriser la scène et tout élément de preuve numérique susceptible d'aider à identifier le responsable de l'incident.

### Dangers liés au drone

**Hélices** – Si elles sont encore en mouvement, recouvrir le drone avec un vêtement lourd ou une couverture afin de l'empêcher de décoller ou de blesser quelqu'un. Si elles ne tournent pas, renverser le drone ou retirer les hélices afin qu'il ne puisse pas décoller.

**Batteries** – Les drones fonctionnent grâce à des batteries LiPo qui peuvent devenir instables si elles sont endommagées ou manipulées de façon inappropriée. Si la batterie est intacte et ne présente aucun signe visible de dommage ou de fuite, la retirer, à condition d'avoir la capacité et l'assurance de pouvoir le faire. En cas de doute, demander conseil.

Tableau 17 - Dangers liés au drone

# LA SÉCURITÉ AVANT TOUT

Les drones représentent des risques particuliers pour les premiers intervenants

Lorsque les rotors ont cessé de tourner, retirer la batterie de l'appareil (si cela ne présente aucun danger) ou renverser le drone.

Ne retirer la batterie que si ses cellules ne semblent ni endommagées ni abîmées, sans quoi il existe des risques de brûlure ou de blessure grave.



Une fois que la batterie est retirée, la placer dans un conteneur sec ou une sacoche spéciale. Une batterie endommagée peut être très instable, et un impact ou la présence d'humidité peut entraîner la rupture ou l'inflammation de ses cellules.

Lorsqu'il est sûr que le drone ne peut pas voler, et si cela ne présente aucun danger, retirer ses hélices.

Noter à quel moment toutes ces opérations sont effectuées.



# LA SÉCURITÉ AVANT TOUT

Les drones représentent des risques particuliers pour les premiers intervenants

- Si le drone est encore en marche, ses rotors peuvent tourner et les hélices en mouvement peuvent causer des blessures à toute personne tentant de saisir l'appareil.
- Si le drone est en marche et que ses rotors tournent, recouvrir l'appareil d'un grand filet ou d'une couverture afin de l'empêcher de décoller et de désactiver les rotors.
- Les batteries LiPo dont sont équipés les drones peuvent être très instables, et un impact ou une fuite des liquides qu'elles contiennent peut provoquer une inflammation ou une explosion.
- Les charges utiles peuvent présenter un danger ou un risque pour les personnes qui les touchent ou se trouvent à proximité.
- Avant d'approcher ou de manipuler un drone sur une scène de crime, le plus important est de prendre des précautions.



Figure 21 : Précautions à prendre lors de la manipulation d'un drone

Les principaux dangers sur un drone proviennent de ses hélices et des batteries LiPo qui assurent son fonctionnement. Chacun de ces éléments requiert des précautions de manipulation afin d'éviter tout risque de blessure.

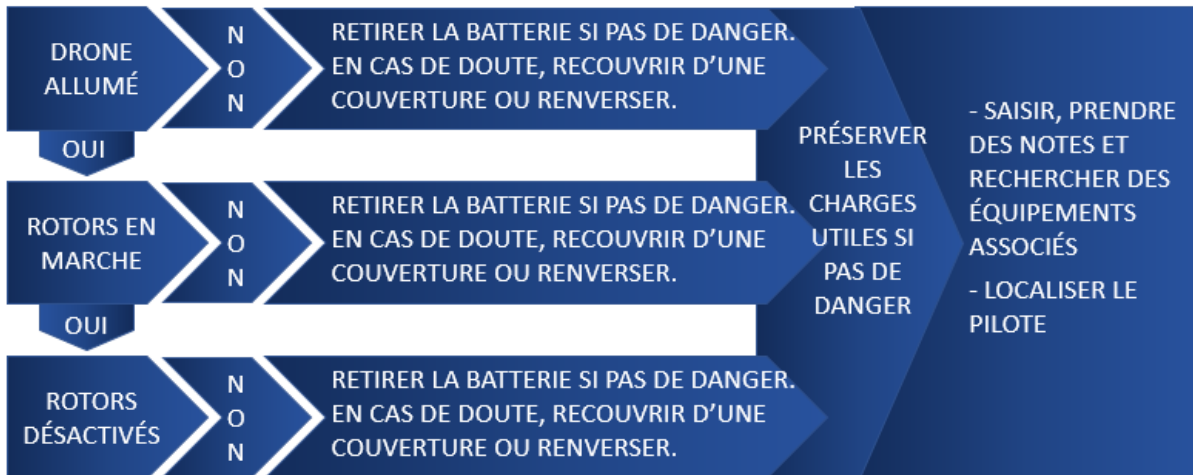


Figure 22 : Consignes de manipulation d'un drone

Figure 23 : Consignes de sécurité d'une batterie LiPo

# PRÉSERVATION

PRÉSERVER LES ÉLÉMENTS DE PREUVE NUMÉRIQUES POUVANT SE TROUVER SUR L'APPAREIL.

DES DONNÉES PEUVENT SE TROUVER SUR UNE CARTE MÉMOIRE OU LA MÉMOIRE INTERNE DE L'APPAREIL.  
IL EST IMPORTANT DE GARDER L'APPAREIL LE PLUS INTACT POSSIBLE.

LORS DE L'EMBALLAGE ET DU TRANSPORT, PROTÉGER L'APPAREIL CONTRE LES IMPACTS OU LES CHOCS. EN CAS DE DÉGRADATION AVANT OU APRÈS LA SAISIE, LE NOTER PAR ÉCRIT.

POUR CONNAÎTRE LES CONSIGNES DE PRÉSERVATION, MANIPULATION ET TRANSPORT DE TOUT AUTRE APPAREIL ÉLECTRONIQUE SAISI, CONSULTER DES ANALYSTES DE CRIMINALISTIQUE NUMÉRIQUE.

EN CAS DE DOUTE. DEMANDER CONSEIL À DES PERSONNES COMPÉTENTES.







Figure 24 : Préservation des éléments de preuve numériques



# SAISIE

## SAISIR TOUS LES ÉQUIPEMENTS

*LES DRONES S'ACCOMPAGNENT GÉNÉRALEMENT D'AUTRES APPAREILS PERMETTANT D'ASSURER LEUR CONTRÔLE ET DE VISUALISER LEUR CONTENU (TÉLÉCOMMANDE, PLATEFORMES D'AFFICHAGE MOBILES TELLES QUE TÉLÉPHONE/ORDINATEUR PORTABLE, TABLETTE, ETC.).*

- Des données de valeur probante peuvent se trouver sur le drone, la télécommande, les appareils mobiles, un ordinateur et les supports de stockage infonuagiques.
- Saisir tout équipement pouvant avoir été associé au drone (télécommande, téléphone/ordinateur portable, ordinateur de bureau, carte mémoire, clé USB, etc.).
- Avant de saisir des équipements associés au drone (en particulier une télécommande et un téléphone portable), LES ÉTEINDRE. Le but est d'empêcher que les données soient effacées à distance et qu'elles ne soient perdues.

**EN CAS DE DOUTE, DEMANDER CONSEIL.**







Figure 25 : Collecte d'éléments de preuve numériques


# RELEVÉ D'INFORMATIONS


**Noter dans quel état se trouve le drone :**

- Allumé/Éteint ?
- Les hélices tournent-elles ?
- Les indicateurs lumineux du drone sont-ils allumés ? Clignotent-ils ?
- Y a-t-il une charge utile ?
- La cible visée est-elle identifiable ?
- Le drone est-il endommagé ou y a-t-il des signes qu'il s'est écrasé ?
- Est-il possible d'identifier le pilote ou d'autres suspects ?

**Quels sont les identifiants du drone ?**

- Numéros de série (du drone et des batteries)
- Référence du modèle
- Numéro de série de l'autorité de l'aviation





**PHOTOGRAPHER :**

- TOUTES LES PARTIES DU DRONE ET LA ZONE ENVIRONNANTE.
- LES DÉGRADATIONS OU MODIFICATIONS QUE PRÉSENTE LE DRONE.
- TOUT ÉQUIPEMENT ASSOCIÉ DÉCOUVERT SUR PLACE.
- SI UN ÉQUIPEMENT ASSOCIÉ EST ALLUMÉ, PHOTOGRAPHER LES DONNÉES AFFICHÉES AINSI QUE LA DATE ET L'HEURE.

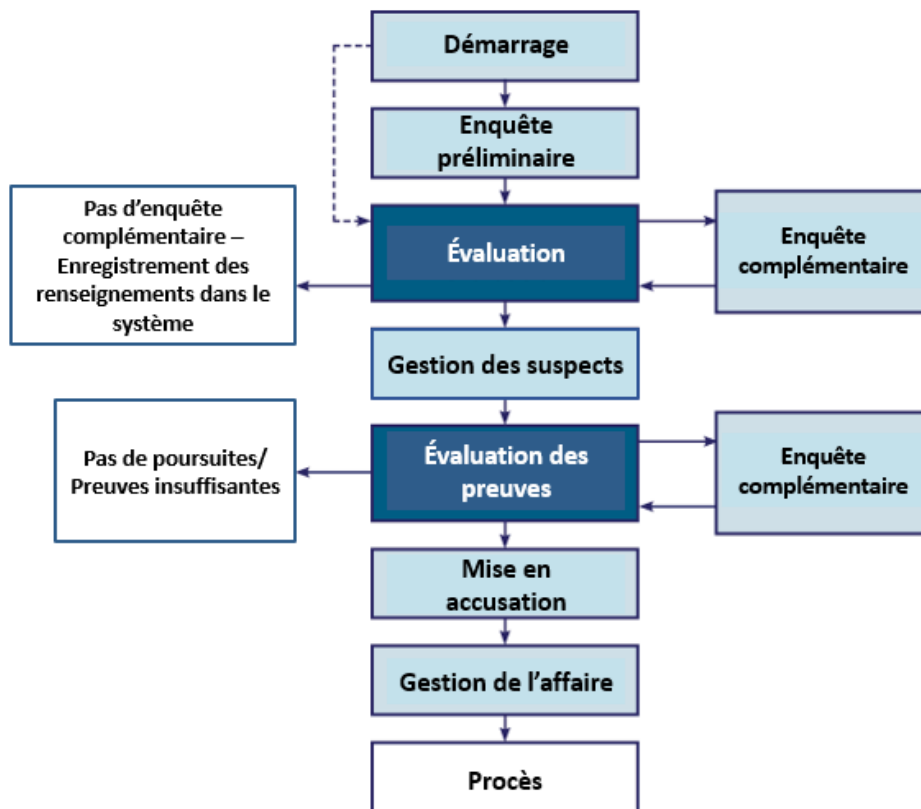
Figure 26 : Relevés d'informations sur la scène de l'incident

### 3.14 Déroulement de l'enquête

Une fois que la scène de crime a été analysée et que toutes les actions requises ont été effectuées, la nécessité est de prouver qui a commis l'infraction, pourquoi, où et quand, et donc d'identifier les suspects et de trouver leurs mobiles.

La façon de procéder des enquêteurs et le type de pièces justificatives recueillies dépendent de la méthode utilisée pour mener l'enquête, à savoir réactive ou proactive. Les étapes sont en revanche similaires, comme le montre le diagramme ci-dessous.

Chaque enquête est différente et peut avoir un déroulement particulier. Dans certains cas, par exemple, l'identité de l'auteur de l'infraction est connue dès le début, et l'enquête passe rapidement à l'étape de gestion des suspects. Dans d'autres, l'identité de l'auteur peut ne jamais être mise au jour, ou seulement à l'issue d'une enquête approfondie.



Les cadres en bleu clair représentent les activités liées à l'enquête, ceux en bleu foncé les principaux points de décision, et ceux en blanc les résultats pouvant être obtenus.

Figure 27 : Vue d'ensemble du déroulement d'une enquête

La phase d'enquête préliminaire a lieu lorsqu'un certain nombre d'actions ont été accomplies :

- Le premier intervenant ou l'enquêteur a obtenu un premier exposé des faits de la part des victimes et des témoins se trouvant sur place.
- Les besoins immédiats des victimes et des témoins ont été satisfaits.
- La scène de crime a été examinée.
- Toutes les actions urgentes relatives aux pièces trouvées sur place ont été réalisées.
- Tous les enregistrements requis par les dispositions en vigueur au niveau local ont été effectués et contrôlés.
- Toutes les informations recueillies lors de l'enquête préliminaire ont été transmises.

Les guides à l'intention des services de police indiquent aux opérateurs du centre d'appels, aux agents de sécurité et aux policiers patrouilleurs quelles informations ils doivent recueillir et les actions qu'ils doivent ensuite entreprendre. Lorsqu'ils recueillent les exposés des faits, les policiers doivent veiller à enregistrer, conserver et mettre en lumière toutes les informations, et à les transmettre à l'enquêteur. Ce dernier doit avoir une bonne connaissance des techniques à employer à l'égard des victimes et des témoins car cela lui permet d'exploiter dès que possible les occasions qui se présentent de collecter des renseignements en questionnant la personne exposant les faits.

Des informations complètes doivent être enregistrées car elles apportent une valeur ajoutée à l'enquête en :

- permettant à l'enquêteur d'évaluer le déroulement de l'enquête ;
- fournissant des renseignements utiles sur le domaine de criminalité concerné ;
- permettant aux superviseurs d'évaluer la qualité de l'enquête ;
- facilitant le transfert éventuel de l'enquête à un autre policier.

### 3.14.1 Enquête complémentaire

Lorsqu'une enquête complémentaire s'avère nécessaire dans le cadre d'une infraction, les enquêteurs doivent réfléchir à la façon dont ils vont s'y prendre pour que l'enquête produise des résultats. Le plan de l'enquête doit s'appuyer sur une évaluation rigoureuse des pièces qui ont déjà été recueillies, et inclure les éléments suivants :

Les trois éléments à prendre en compte avant de lancer une enquête complémentaire
<ul style="list-style-type: none"> <li>• Les objectifs spécifiques de l'enquête complémentaire ;</li> </ul>
<ul style="list-style-type: none"> <li>• Les stratégies à utiliser pour atteindre ces objectifs ;</li> </ul>
<ul style="list-style-type: none"> <li>• Les ressources requises pour mener cette enquête : enquêteur, technicien de scène de crime, expert en criminalistique numérique et analyste de renseignements.</li> </ul>

Tableau 18 - Les trois éléments à prendre en compte avant de lancer une enquête complémentaire

Bien que non exhaustives, les considérations ci-dessus visent à guider l'enquêteur. Les stratégies à utiliser ne sont pas abordées dans le présent Cadre, car cela dépasse son champ d'observation.

Pour revenir au diagramme du déroulement d'une enquête, nous avons abordé jusqu'ici les phases d'enquête préliminaire et d'évaluation. Les sections suivantes décrivent l'évaluation des éléments de preuve et autres processus intervenant dans les enquêtes portant sur les incidents liés à un drone. La section suivante porte sur la stratégie en matière de criminalistique numérique et les opérations d'analyse des données relatives aux drones, afin de permettre aux premiers intervenants et aux professionnels de la criminalistique numérique de comprendre le processus.

## 4. PRESENTATION GENERALE ET PRINCIPES DE LA CRIMINALISTIQUE NUMERIQUE

### 4.1 Présentation générale

La criminalistique numérique est une branche de la police scientifique qui se concentre sur le repérage, l'acquisition, le traitement, l'analyse et le compte rendu des données stockées sur un ordinateur, un appareil électronique ou tout autre support de stockage numérique. L'objectif de cette discipline est d'extraire des données des pièces à conviction électroniques, de traiter ces informations pour les rendre exploitables, et de soumettre les résultats à la justice. Pour que ces résultats soient recevables par un tribunal, tous les processus précités doivent faire appel à des techniques criminalistiques éprouvées.

L'utilisation de la criminalistique numérique sur les drones et équipements associés a pour but d'en savoir plus sur les itinéraires de vol et sur l'utilisateur, ainsi que de mettre au jour les photos et vidéos enregistrées sur les appareils, afin de mieux comprendre l'usage qui est fait desdits drones.

Les affaires faisant apparaître des éléments de preuve numériques sont généralement transfrontières et les faits sont très rapides. Les résultats du traitement de ces éléments doivent par conséquent être obtenus en respectant un ensemble de consignes normalisées, afin qu'ils soient recevables non seulement dans le système judiciaire d'un pays particulier, mais aussi dans le système de justice pénale international.

Les chapitres suivants décrivent les bonnes pratiques en matière de manipulation des UAV, applicables pour tous les types de drones – récréatifs, commerciaux et sur mesure – et contrôleurs de vol. Chacun de ces chapitres fournit des informations contextuelles, notamment des instructions pas à pas claires et concises sur la législation et les infractions concernant les UAV. Ils comprennent en outre une section expliquant comment gérer un drone et en préserver l'intégrité, depuis le premier contact jusqu'à son examen sommaire ou plus poussé par la police scientifique.

Il est très important pour un enquêteur de comprendre que si les renseignements et les éléments de preuve numériques doivent être traités différemment, les mêmes principes doivent être appliqués aux uns et aux autres pendant tout le processus de gestion de l'affaire, depuis la phase de saisie jusqu'au procès devant un tribunal.

## 4.2 Principes des éléments de preuve électroniques



Figure 28 : Analystes de criminalistique numérique examinant un drone

Lorsque l'on est en présence d'éléments de preuve électroniques, les principes à respecter sont les suivants :

Principes applicables aux éléments de preuve numériques	
<b>Principe N° 1</b>	Les éléments de preuve numériques doivent être obtenus de façon légale.
<b>Principe N° 2</b>	Les personnes chargées d'examiner les éléments de preuve électroniques doivent recevoir préalablement une formation appropriée.
<b>Principe N° 3</b>	Aucune des actions effectuées sur les éléments de preuve numériques ne doit entraîner la modification des données. S'il est nécessaire d'accéder aux données d'origine ou de modifier la configuration du système, seul le personnel compétent doit le faire, et être capable de justifier ce qu'il fait.
<b>Principe N° 4</b>	Toutes les actions effectuées lors de la manipulation des éléments de preuve numériques doivent être consignées dans un registre qui doit être conservé afin de pouvoir être contrôlé. Une tierce partie indépendante doit pouvoir répéter les mêmes actions et obtenir le même résultat.

Tableau 19 - Principes de base applicables aux éléments de preuve numériques

La conclusion est que la saisie du drone et des équipements associés est cruciale si l'on veut que les éléments de preuve numériques soient exploités du mieux possible.

### 4.3 Présentation générale d'un laboratoire de criminalistique numérique

Lorsque le drone et les équipements associés sont soumis à un laboratoire de criminalistique numérique, celui-ci doit avoir une procédure de gestion préétablie. En règle générale, cette procédure comporte sept étapes, comme cela est illustré sur la figure ci-dessous et expliqué dans les sections qui suivent. Avant de s'occuper d'un dossier, le laboratoire de criminalistique numérique doit s'assurer qu'il respecte la législation. Le directeur ou l'analyste doit vérifier qu'ils ont reçu des mandats ou documents officiels autorisant le traitement des éléments de preuve. Le travail du laboratoire consiste à utiliser ces éléments de preuve pour confirmer ou informer des faits contestés, raison pour laquelle il est important que les éléments de preuve électroniques soient obtenus en respectant la législation. Lorsque le travail du laboratoire est terminé, il convient de s'assurer que les éléments de preuve électroniques et le rapport résultant de leur analyse sont recevables devant un tribunal.



Figure 29 : Processus de travail d'un laboratoire de criminalistique numérique

#### 4.3.1 Réception de la demande

La mission du laboratoire de criminalistique numérique démarre lorsque celui-ci reçoit une demande formelle, qui peut lui être envoyée par courrier, message électronique ou télécopie. Les informations contenues dans cette demande sont notamment l'infraction concernée, la loi applicable, les détails concernant les éléments de preuve électroniques, l'objectif de la demande et éventuellement le mandat.

Le directeur du laboratoire ou le personnel désigné examine la demande et détermine si elle peut être satisfaite, en s'appuyant sur les critères suivants :

- a) Le dossier relève bien du domaine de la criminalistique numérique (les éléments de preuve sont bien électroniques et pas d'une autre nature, comme par exemple de l'ADN ou des empreintes digitales).
- b) Les méthodes et les outils sont disponibles.
- c) Le personnel est disponible pour s'en occuper.
- d) Les dispositions légales sont respectées.

Le laboratoire répond ensuite à la demande de manière formelle, que ce soit pour l'accepter ou la décliner. S'il accepte la demande, le laboratoire fournit au demandeur une date de restitution des éléments de preuve.

#### 4.3.2 Enregistrement du dossier

Une fois que le laboratoire de criminalistique numérique a décidé que la demande pouvait être satisfaite, le demandeur doit s'y rendre pour lui remettre les éléments de preuve numériques. Le laboratoire crée alors un numéro de dossier unique et remplit un formulaire.

Pour pouvoir examiner efficacement les éléments de preuve, les analystes ont besoin que la demande soit claire et précise, car un appareil peut contenir une grande quantité et diversité de données (documents, vidéos, communications, données médicales, lieux, etc.).

Grâce aux précisions fournies par le demandeur, l'analyste peut prévoir les méthodes et les outils qu'il utilisera pour analyser les preuves.

Les deux parties – le demandeur et le laboratoire de criminalistique numérique – signent alors le formulaire. La mission est désormais officielle. Le laboratoire crée ensuite un dossier électronique sur un support de stockage, dans lequel il enregistrera toutes les données relatives au travail qui lui a été confié.

#### **4.3.3 Enregistrement des pièces à conviction**

Lorsque les éléments de preuve électroniques (ou pièces à conviction) sont transmises au laboratoire de criminalistique numérique, il est important qu'elles soient placées dans un scellé. Afin d'enlever tout doute raisonnable concernant l'intégrité des éléments de preuve, le demandeur comme l'analyste doivent être en mesure de démontrer que personne n'y a eu accès pendant le transfert entre les deux parties. Bien que cette pratique soit nouvelle et coûteuse pour certains services, le laboratoire leur en fait part et indique la date précise à partir de laquelle elle est mise en place.

Chaque élément de preuve électronique qui est confié au laboratoire doit être enregistré et étiqueté à l'aide d'un numéro unique. Ce numéro est retranscrit, avec la description de la pièce à conviction, sur le formulaire d'enregistrement.

Tous les composants de chaque pièce à conviction (comme les cartes SIM et les cartes mémoire) doivent également être enregistrés. Les numéros figurant sur les étiquettes doivent permettre d'établir le lien entre la pièce à conviction et ses différents composants. Par exemple, si un téléphone portable est numéroté 20190105(2)-MP01, sa carte SIM portera par exemple le numéro 20190105(2)-MP01-SIM01.

Il est important de noter que les défauts que peuvent présenter les pièces à conviction doivent être précisés sur le formulaire d'enregistrement. Cela permet, en cas de plainte ultérieure, de protéger le laboratoire.

Tout document numérique se rapportant à une pièce à conviction doit être enregistré dans le dossier électronique.

La chaîne de conservation des pièces à conviction est désormais créée, et le formulaire d'enregistrement doit être rempli par le personnel prenant possession de ces pièces.

#### **4.3.4 Photographie des pièces à conviction**

Les raisons pour lesquelles les pièces à conviction doivent être photographiées sont les suivantes : garder une trace de l'état dans lequel elles se trouvent ; pouvoir les reconnaître à l'avenir. Ces photos doivent donner une vue d'ensemble, mais aussi de près, de chaque pièce. S'il s'agit d'un écran en état de marche, photographier également son affichage. Les photos doivent ensuite être enregistrées dans le dossier électronique. Il est recommandé de photographier les pièces avant de les restituer au demandeur afin de se rappeler ultérieurement de leur état.

#### **4.3.5 Analyse**

L'analyse doit avoir lieu conformément au modèle mis en place par le laboratoire de criminalistique numérique. Pour en savoir plus sur le déroulement de l'analyse, se reporter à la section 5. Au cours de ce processus, les analystes doivent rester en contact avec le demandeur et lui faire part de tout problème pouvant survenir. Certains analystes ont plusieurs années d'expérience dans la criminalistique numérique et sont donc capables, lorsque la communication avec le demandeur est efficace, de trouver les bonnes données.

#### 4.3.6 Restitution des pièces à conviction

Une fois l'analyse terminée, le laboratoire de criminalistique numérique contacte le demandeur pour qu'il récupère les éléments de preuve. De manière générale, le laboratoire restitue les pièces à conviction en même temps qu'il remet les résultats de l'analyse au demandeur, afin de gagner du temps. Avant de restituer les pièces à conviction, le laboratoire les place dans un sac scellé. Celui-ci doit comporter les initiales de l'analyste, le numéro de chaque pièce ainsi que la date et l'heure de fermeture du scellé.

#### 4.3.7 Clôture du dossier

Le processus est alors terminé et le laboratoire de criminalistique numérique peut clore le dossier. Les deux parties conviennent que le travail est achevé et que les résultats ont été remis au demandeur. Elles peuvent pour cela signer un formulaire.

## 5. ANALYSE CRIMINALISTIQUE NUMERIQUE D'UN DRONE

Ce chapitre décrit le processus d'analyse criminalistique numérique d'un drone et de sa télécommande. Si d'autres équipements sont associés au drone (ordinateur/téléphone portable ou tablette), le processus correspondant est expliqué dans les Principes directeurs d'INTERPOL liés aux laboratoires de criminalistique numérique.

### 5.1 Présentation générale

Ce chapitre décrit le processus d'analyse des éléments de preuve numériques liés à un drone qui est mené à bien dans un laboratoire de criminalistique numérique. Un modèle chronologique est présenté ici afin de donner une vue d'ensemble des principales tâches intervenant dans ce processus.

L'analyse criminalistique des éléments de preuve numériques comporte généralement quatre phases : acquisition, examen, analyse et présentation. Pendant toute la durée du processus, la chaîne de conservation doit être actualisée chaque fois que les éléments de preuve changent de mains, et l'intégrité des preuves doit être en permanence préservée. Les phases d'examen et d'analyse peuvent être répétées jusqu'à ce qu'elles donnent des résultats correspondant à la demande.

S'il est communément admis que le processus d'analyse criminalistique numérique comprend généralement ces quatre phases, ce n'est en fait pas toujours le cas. Il arrive que la phase d'acquisition soit supprimée pour passer directement à l'examen. C'est le cas, par exemple, lorsque les données sont très nombreuses et qu'il n'est pas forcément faisable de procéder à l'acquisition de chacune d'elles.

La figure ci-dessous représente le modèle chronologique suivi par le laboratoire pour procéder à l'analyse :

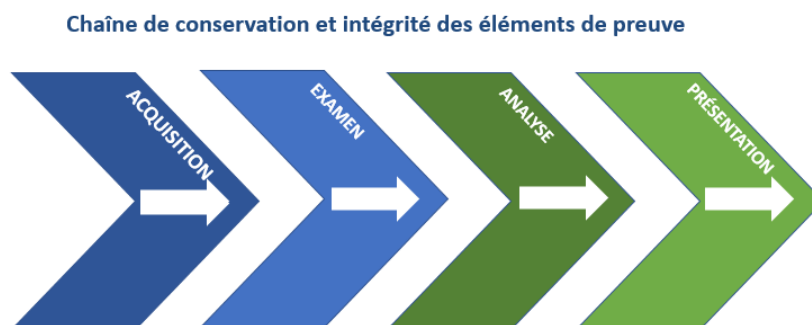


Figure 30 : Modèle d'analyse criminalistique numérique



### 5.1.1 Les drones et leurs équipements

Les sections qui suivent décrivent en détail chaque étape du processus d'analyse mené à bien par un laboratoire de criminalistique numérique sur deux types d'appareils :

- I) Les drones ;
- II) Leurs télécommandes.

Comme expliqué à la section 2.5 du présent document, un drone génère plusieurs types de données qui sont stockées sur différents supports (le drone lui-même, des supports amovibles, des appareils mobiles, le nuage, etc.). On a vu qu'il pouvait aussi y avoir des données résiduelles sur la télécommande du drone. L'analyste peut, si besoin, essayer de récupérer des données sur la télécommande. Ces données peuvent être les suivantes :

Types de données stockées sur la télécommande d'un drone	
<b>Données télémétriques</b>	Données se rapportant aux vols effectués par le drone : géolocalisation, date et heure (provenant du signal GPS), vitesse, direction, altitude, vitesse de rotation du moteur et informations saisies par l'utilisateur.
<b>Équipements associés</b>	Tout appareil associé ou connecté à la télécommande (comme un téléphone portable ou une tablette). On peut trouver le numéro IMEI de cet appareil ou son identifiant unique.
<b>Compte d'utilisateur enregistré</b>	Il peut s'agir d'une adresse de messagerie électronique enregistrée ou d'un nom de compte ayant été créé auprès du fabricant du drone.
<b>Paramètres de communication entre le drone et la télécommande</b>	Données de signalisation mémorisant la puissance du signal entre le drone et la télécommande.

Tableau 20 - Types de données stockées sur la télécommande d'un drone

Pour des consignes concernant spécifiquement l'analyse criminalistique numérique d'autres équipements associés à un drone (comme un téléphone portable ou un ordinateur), se reporter aux Principes directeurs d'INTERPOL liés aux laboratoires de criminalistique numérique.

## 5.2 Acquisition

L'acquisition – ou, plus précisément, l'acquisition de données – est le processus consistant à créer sous la forme d'un ou de plusieurs fichiers images, la copie numérique d'un élément de preuve (pièce à conviction) électronique (comme le contenu du drone, de sa télécommande, d'un téléphone ou d'un ordinateur portable). Ces fichiers images sont ensuite utilisés lors de la phase d'analyse. L'acquisition a pour but de préserver l'intégrité des éléments de preuve d'origine, en produisant une copie identique des données sans en modifier d'aucune manière le contenu. Il est recommandé de créer deux copies, l'une conservée en tant que fichier maître, et l'autre utilisée pour l'analyse criminalistique.

L'acquisition des éléments de preuve électroniques doit avoir lieu selon une méthode éprouvée. De par leur caractère intangible, les données et les informations stockées sur des supports électroniques sont faciles à manipuler et plus sujettes à l'altération que des formes d'éléments de preuves plus classiques. Il est donc important de disposer d'une procédure préétablie ayant fait ses preuves.

Une fois que le fichier image a été créé, il convient d'enregistrer la signature numérique de ce fichier et de la pièce à conviction. Cette signature permet de prouver que le fichier reflète exactement le contenu de la pièce à conviction. Elle peut être obtenue à l'aide de nombreux algorithmes de hachage employés dans le domaine de la criminalistique numérique, comme SHA-256. La plupart des logiciels et des matériels utilisés dans ce domaine comportent des fonctions de hachage.

L'examen et l'analyse doivent obligatoirement être effectués sur une copie numérique des éléments de preuve, sauf si les circonstances ne le permettent pas. Cela est important pour préserver l'intégrité des preuves. La copie numérique doit être enregistrée sur un support de stockage distinct, et non sur l'appareil constituant la pièce à conviction. Elle doit être clairement étiquetée, de manière à ne pas être confondue avec l'original de l'élément de preuve ou avec les copies numériques d'autres dossiers. Le laboratoire de criminalistique numérique doit donc, avant de recevoir des demandes d'analyse, préparer des supports de stockage.

La section suivante décrit en détail les méthodes d'extraction des données utilisées pour les drones. Elles sont très similaires à celles employées pour les téléphones portables, car les procédures d'examen de ces deux types d'appareils présentent des points communs.

### 5.2.1 Méthodes d'extraction des données

Avant de commencer à travailler, l'analyste de criminalistique numérique consulte les documents fournis par le demandeur afin de déterminer quels types de données doivent être extraites de la pièce à conviction. Cela peut l'aider à décider quelle est la méthode d'extraction la plus adaptée.

Il existe pour les drones quatre niveaux d'extraction différents, qui sont décrits ci-après en commençant par celui qui permet d'extraire le plus de données.



Figure 31 : Drone en cours d'examen

#### a) Extraction physique

Cette tâche consiste à extraire de l'espace de stockage de l'appareil des données binaires brutes. Ces données sont ensuite analysées et traitées par un logiciel d'analyse criminalistique. Cette méthode permet généralement à l'analyste d'avoir accès à des données actives ou supprimées, aux fichiers du système d'exploitation et à des emplacements de l'appareil qui ne sont normalement pas accessibles par l'utilisateur.

#### b) Vidage système des fichiers

Le vidage système des fichiers, qui est une méthode hybride entre l'extraction physique et l'extraction logique, consiste à récupérer des fichiers se trouvant sur le système de l'appareil et à interpréter les données au cours de la phase de traitement. Grâce à ce procédé, l'analyste peut par exemple retrouver des bases de données télématiques/multimédias qui ne seraient peut-être pas disponibles dans le cas

d'une extraction logique et pas accessibles lors d'une extraction physique. L'inconvénient du vidage système des fichiers est qu'il ne permet pas, contrairement à l'extraction physique, de récupérer toutes les données supprimées.

#### *c) Extraction logique*

L'extraction logique consiste à réceptionner les données provenant du drone et à autoriser l'appareil à soumettre les données à l'analyse. Elle équivaut souvent à accéder aux données directement depuis l'appareil. Avec cette méthode, seules les données actives sont accessibles par l'analyste. Cette fonctionnalité est disponible sur la plupart des logiciels d'analyse criminalistique, à condition que les données ne se trouvent pas sur une carte amovible. Le problème avec l'extraction logique est qu'il n'y a aucun moyen de vérifier les données sur le drone lui-même, car la plupart de ces engins ne possèdent pas d'écran pour visualiser leurs données.

#### *d) Retrait de la puce mémoire*

Pour les drones qui sont équipés d'une mémoire intégrée ou qui sont endommagés, la méthode du retrait de la puce peut être utilisée pour extraire les données. Elle permet également d'extraire des données binaires brutes de la mémoire du drone, mais nécessite pour cela le retrait permanent de la puce de la carte mémoire de l'appareil. Le retrait de la puce est une opération qui risque d'endommager l'appareil et de le mettre hors d'usage. Par ailleurs, il convient de ne pas avoir d'attentes excessives quant aux résultats de cette méthode, car les modèles récents de drones renferment sur leur puce mémoire des données cryptées.

S'agissant des télécommandes de drones, l'analyste doit repérer la puce mémoire sur la carte de l'appareil, puis extraire les données à l'aide d'une connexion USB ou de la technologie JTAG, ou du retrait de la puce. Une télécommande peut aussi comporter des cartes amovibles, qui doivent être traitées comme n'importe quel support amovible.

L'ordre dans lequel les méthodes d'extraction sont utilisées a son importance. Il convient de choisir la technique qui cause le moins de dégâts mais permet de récupérer le maximum de données. Elle doit aussi permettre d'accéder à des emplacements qui risquent ultérieurement d'être endommagés ou dont le contenu pourra être écrasé. Une méthode comme le retrait de la puce mémoire ne doit être envisagée qu'en dernier ressort, car le procédé peut entraîner des dégâts irréversibles.

L'utilisation de la technologie JTAG peut causer des problèmes, en particulier sur les marques de drones à succès. Cette méthode doit être testée au préalable sur un autre appareil que la pièce à conviction, car elle risque de rendre le microcontrôleur hors service et d'empêcher d'y récupérer quelque donnée que ce soit.

### **5.2.2 Outils d'extraction**

L'analyse criminalistique d'un drone nécessite généralement un logiciel spécialisé, des câbles d'alimentation et des câbles de transfert de fichiers. Les techniques plus complexes, comme le retrait de la puce mémoire, requièrent des outils supplémentaires, par exemple pour dessouder/ressouder et lire les données brutes sur les cartes mémoire des appareils. Il peut aussi être nécessaire d'utiliser les suites logicielles des fabricants – même si elles ne relèvent pas du domaine de la criminalistique –, lorsque ce sont les seuls moyens disponibles pour extraire les données.

### **5.2.3 Format des fichiers d'extraction**

Compte tenu de la nécessité d'utiliser des outils spécialisés, les données extraites des drones le sont souvent au format propriétaire. Les fichiers correspondants sont souvent transférés d'un outil à un autre afin d'exploiter au mieux les points forts des différentes fonctionnalités de décodage. Les formats non propriétaires sont par exemple BIN et RAW.

## 5.2.4 Processus d'extraction



Figure 32 : Processus d'extraction des données contenues sur les drones et leurs télécommandes

### a) Identifier la pièce à conviction et un support de stockage

L'analyste de criminalistique numérique examine la pièce à conviction qui lui a été confiée avant de passer à l'étape suivante.

#### i) Drone

L'étiquette est apposée sur le drone, que ce soit sur sa face interne ou au dos. Elle peut indiquer le nom du fabricant, la référence du modèle, le numéro de série et l'identifiant du réseau wifi (SSID).

#### ii) Télécommande

L'étiquette est fixée au dos de la télécommande, ou à l'intérieur du compartiment où se trouve la batterie. Elle indique le nom du fabricant, la référence du modèle, le numéro de série et le code d'appariement. La télécommande peut aussi utiliser un système d'exploitation (comme Android), auquel cas il convient d'appliquer les mêmes principes que pour l'examen des appareils mobiles.

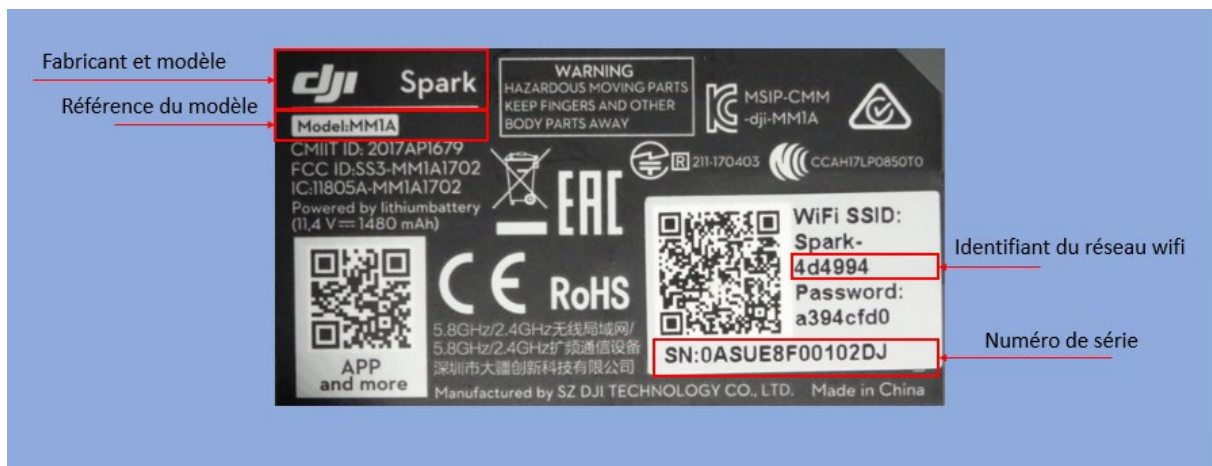


Figure 33 : Étiquette d'identification d'un drone

Après quoi, un support de stockage doit être préparé pour y placer les données issues de l'extraction.

### b) Isoler la pièce à conviction du réseau

Lors de l'extraction des données, l'appareil doit être mis en marche.

#### i) Drone

Pour éviter qu'il ne tente de se connecter à un réseau – ce qui risquerait de modifier les données qu'il contient –, le drone doit être isolé de tout réseau ou de toute autre connexion, par exemple avec le téléphone portable qu'il utilisait.

*ii) Télécommande*

Afin d'éviter qu'elle ne tente de se connecter à un satellite de géopositionnement ou à l'appareil avec lequel elle était associée (comme le drone ou un téléphone portable) – ce qui risquerait de modifier les données qu'elle contient –, la télécommande doit être isolée de tout satellite et des autres appareils. Le but est d'empêcher qu'elle ne capte des signaux (GPS/WIFI ou réseau) et que de nouveaux fichiers/données ne soient créés, révélant la localisation du laboratoire de criminalistique numérique.

Selon le budget disponible, différentes méthodes peuvent être utilisées pour isoler la pièce à conviction :

<b>Méthodes pour isoler la pièce à conviction (drone/télécommande)</b>	
<b>Pièce protégée des ondes</b>	Le laboratoire est conçu comme une cage de Faraday afin d'empêcher la captation des signaux. Cette solution est cependant très coûteuse, et une alternative efficace peut être l'utilisation de petites sacoches de Faraday.
<b>Équipement sans fil/de brouillage des signaux</b>	Cet équipement bloque les signaux GPS/wifi/des réseaux mobiles entrants. Il est cependant interdit dans certains pays. Il aura en outre pour effet de perturber les autres appareils nécessitant ces types de signaux pour envoyer et recevoir des données.
<b>Méthode manuelle</b>	<p>C'est la méthode la moins coûteuse et la plus facile à mettre en œuvre. Il suffit d'utiliser une feuille en aluminium que l'on dispose sur les antennes du drone/de la télécommande pour entraver leur réception des signaux satellite. La méthode n'est cependant pas infaillible car il faut s'assurer que les antennes et la partie située autour sont totalement recouvertes.</p> <p>Il est important de noter que lorsque le drone est mis en route, il essaie au départ de capter un signal GPS pour obtenir sa position, la date et l'heure. Ces informations peuvent être utilisées pour vérifier l'authenticité des données qu'il contient (par exemple, une base de données sur les zones d'interdiction de survol). Par conséquent, chaque fois que le drone est mis en route, un nouveau fichier de données peut être généré dans son système, et apparaître lors de l'examen de l'appareil.</p>

Tableau 21 - Méthodes pour isoler la pièce à conviction (drone/télécommande)

*c) Extraire les données pertinentes*

L'utilisation de certaines techniques d'extraction, de certains appareils de débridage et de drones/télécommandes équipés d'un logiciel semblable aux systèmes d'exploitation mobiles (en particulier Android) fait qu'il n'est pas toujours possible d'empêcher l'écriture de données sur le système du drone ou de la télécommande. Il convient, si possible, de bloquer le processus d'écriture, par exemple sur les cartes mémoire. Toutefois, comme chacun le reconnaît, ce n'est pas toujours faisable ni facile sur les drones et leurs télécommandes. Il est donc impératif que l'analyste de criminalistique numérique ait parfaitement conscience des conséquences de ses actes lorsqu'il manipule des drones/télécommandes, et qu'il soit en mesure de les expliquer et de les justifier.

Les drones/télécommandes sont équipés de deux types de dispositifs de stockage nécessitant des techniques de manipulation distinctes, comme le montre le tableau ci-dessous.

Dispositifs de stockage sur les drones/télécommandes	
Dispositifs	Description
<b>Cartes mémoire</b>	L'examen de ces cartes peut se faire comme celui d'un disque dur d'ordinateur. Les deux types d'extraction – logique et physique – peuvent y être pratiquées, si tant est que les outils de police scientifique utilisés soient dotés de cette fonctionnalité. Le processus consiste à accéder à la carte, à extraire les données, puis à replacer la carte dans l'appareil avant de le mettre en marche. Certains appareils stockent les données sur la carte mémoire, et s'ils détectent que la carte n'est pas accessible, cela peut entraîner une perte de données. Si le temps et les ressources le permettent, un clone de la carte peut être réalisé bit par bit, puis inséré dans l'appareil.
<b>Mémoire interne</b>	L'opération nécessite des outils de police scientifique/du fabricant compatibles avec le drone/l'appareil mobile. L'extraction physique est réalisée, pour certains appareils, à l'aide d'outils de police scientifique qui démarrent l'appareil de façon particulière et procèdent à l'extraction sans modifier ni altérer les données de l'utilisateur qui s'y trouvent.

Tableau 22 - Dispositifs de stockage sur les drones/télécommandes

Traces numériques pouvant se trouver sur un drone/une télécommande	
Ces données sont créées sur le drone/la télécommande par défaut. La probabilité d'en trouver est forte, même si l'utilisateur essaie de les masquer. Ces traces numériques peuvent être les suivantes :	
Traces se trouvant sur des pièces à conviction numériques standard :	Traces se trouvant spécifiquement sur les drones :
<ul style="list-style-type: none"> <li>• Espace de marge.</li> <li>• Espace non alloué.</li> <li>• Cache des miniatures.</li> <li>• Fichiers journaux.</li> </ul>	<ul style="list-style-type: none"> <li>• Historique mis à jour.</li> <li>• Journaux de diagnostic.</li> <li>• Comptes de messagerie électronique enregistrés.</li> <li>• Appareils associés.</li> <li>• Fichiers multimédias.</li> <li>• Journaux de vol/télématiques.</li> <li>• Fichiers cache des miniatures.</li> <li>• Traces cartographiques (coordonnées GPS, points de passage et positions d'origine).</li> <li>• Logiciel spécifique au drone, comme le gestionnaire du fabricant.</li> <li>• Messages électroniques concernant l'enregistrement du drone ou des avis de mise à jour du fabricant.</li> <li>• Fichiers CSV contenant des données télématiques, des diagnostics ou des coordonnées GPS.</li> </ul>

Tableau 23 - Traces numériques pouvant se trouver sur un drone/une télécommande

Le processus d'extraction varie selon l'outil choisi. La plupart des outils de police scientifique s'accompagnent d'un guide expliquant la procédure. Dans certains cas, l'extraction des données nécessite de modifier au préalable les fichiers système ou le système d'exploitation de l'appareil. Bien que cette opération puisse causer la perte irréversible de certaines données, elle ne touche en réalité que des fichiers système sans grande utilité probante. L'un des moyens de connaître les altérations



causées par cette opération peut être de suivre une formation spécifique (par exemple celle dispensée par les fabricants de logiciels de police scientifique applicables aux drones/appareils mobiles), ou d'acquérir une expérience pratique avec des exercices d'extraction sur un drone/appareil mobile.

D'autres sources substantielles d'éléments de preuve sont les fichiers de sauvegarde, de diagnostic et de données télémétriques du drone. Certains drones et équipements associés créent des sauvegardes ou des copies sur d'autres périphériques (par exemple un ordinateur) ou sur le nuage. Ces sauvegardes peuvent permettre de reconstituer une chronologie, et également d'accéder à des données historiques qui ne se trouvent pas sur le drone. Certaines d'entre elles peuvent aussi être analysées comme s'il s'agissait d'un appareil physique.

Du fait de la nature même des drones/télécommandes, les outils de police scientifique standard peuvent ne pas permettre d'extraire et d'analyser les données qui s'y trouvent. Il peut alors être nécessaire d'utiliser un logiciel du commerce. Dans ce cas, il est conseillé d'effectuer des vérifications et des contrôles qualité afin de s'assurer que les données récupérées sont conformes, ainsi que d'évaluer préalablement quel sera l'impact de cette opération sur la pièce à conviction. Par ailleurs, en cas d'utilisation d'un logiciel conçu par le fabricant du drone, il faut être conscient que l'application risque d'envoyer des données ou des copies des fichiers récupérés sur les serveurs du fabricant pour information.

#### *d) Vérifier la pièce à conviction et les données extraites*

Une fois que les données ont été extraites, il convient de les comparer avec celles se trouvant sur la pièce à conviction. Les informations telles que la date et l'heure, les coordonnées GPS et l'identifiant de l'utilisateur/du système doivent faire l'objet d'une vérification croisée de la part de l'analyste, car il arrive que leur format soit modifié au cours de l'extraction. Étant donné que les drones ne possèdent pas d'interface utilisateur permettant de consulter les données se trouvant sur l'engin, il est recommandé, dans la mesure du possible, que les données soient extraites et analysées par deux outils de police scientifique au moins. On appelle cela le double outillage.

#### *e) Consigner toutes les actions*

La dernière étape de l'acquisition des données contenues sur un drone/une télécommande consiste à conserver une trace écrite du processus. L'analyste doit prendre des notes lors de l'acquisition des données, en indiquant la date et l'heure de ses actions, le logiciel utilisé (de police scientifique ou autre), ainsi que toute erreur ou anomalie survenue au cours du processus. Il s'agit d'une opération essentielle pour la chaîne de conservation des preuves, qui est également requise en cas de présentation des éléments de preuve devant un tribunal. L'analyste doit garder à l'esprit qu'il peut se passer beaucoup de temps entre les étapes d'acquisition, d'examen et d'analyse des données et les poursuites judiciaires, et que ses notes doivent donc être les plus complètes possible.



# DRONE

## Examen préliminaire

- Déterminer la marque et le modèle du drone.
- Photographier le drone et relever les dégâts éventuels.
- Retirer la batterie et vérifier si elle est endommagée ou gonflée.

## Retirer les hélices

- Étiqueter chaque hélice en notant sur quel(le) bras/aile elle était fixée.
- Noter et photographier les dégradations éventuelles sur chaque bras/aile ou hélice.

## Procéder à l'acquisition de données sur les supports de stockage externes

- Vérifier si le drone comporte des supports de stockage externes (des cartes mémoire, par exemple).
- Photographier et étiqueter ces supports.
- Réaliser une image physique de ces supports en utilisant un logiciel/matériel de police scientifique approprié.

## Procéder à l'acquisition de données sur la mémoire interne

- Connecter le drone à un outil de police scientifique et procéder à l'acquisition de données en utilisant un logiciel/matériel approprié de la police scientifique/du fabricant.
- Charger complètement la batterie du drone avant de lancer l'acquisition.

# Méthodes d'acquisition

### Connexion USB

- Connecter à un ordinateur de bureau.
- Procéder à l'acquisition en utilisant un logiciel/matériel approprié.

### JTAG

- Localiser les connecteurs JTAG.
- Connecter un boîtier JTAG pour récupérer les données.

### Programmation in-situ (ISP)

- Localiser les points de raccordement ISP.
- Procéder à l'acquisition des données.

### Retrait de la puce mémoire

- Localiser la puce mémoire.
- La retirer, la nettoyer et, si nécessaire, procéder à son rebillage.
- Réaliser une image à l'aide d'un adaptateur et d'un outil de programmation appropriés.

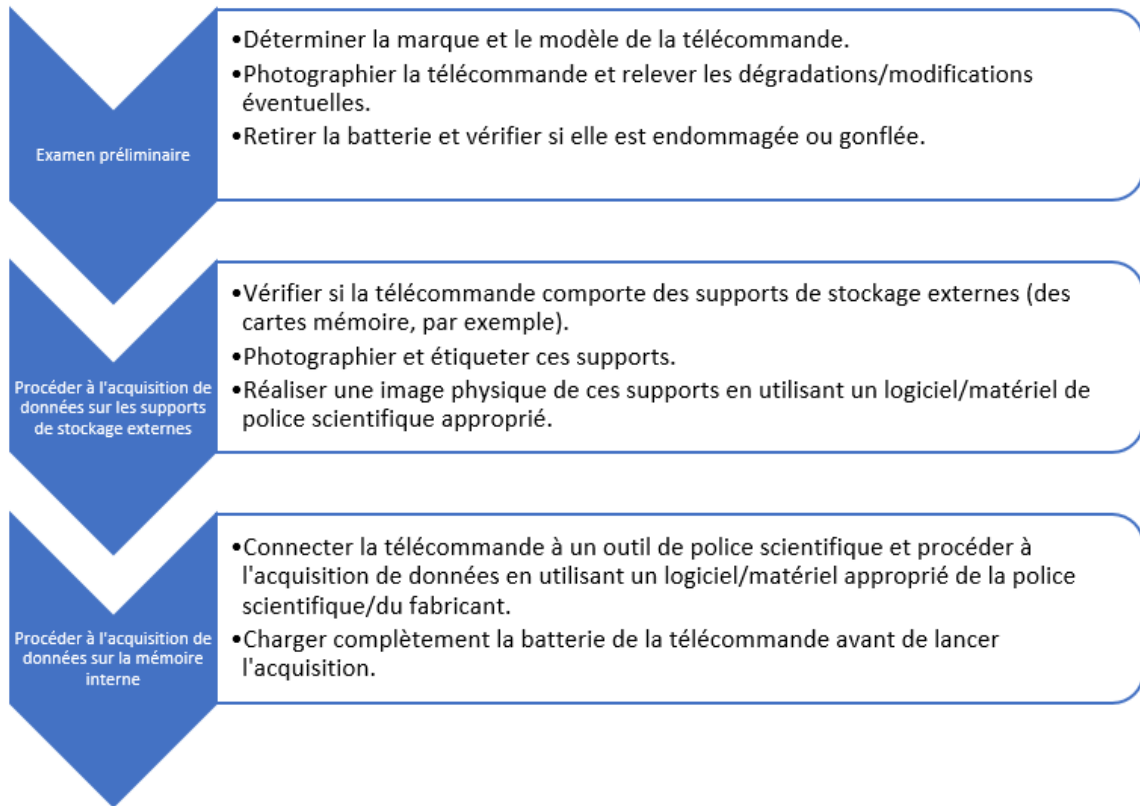
## Réviser et valider les résultats

- Analyser et vérifier les résultats.
- Établir un rapport présentant les résultats et les observations.

Figure 34 : Diagramme récapitulatif de l'examen d'un drone



## Télécommande



## Méthodes d'acquisition

Connexion USB	JTAG	Programmation in-situ (ISP)	Retrait de la puce mémoire
<ul style="list-style-type: none"> <li>• Connecter à un ordinateur de bureau.</li> <li>• Procéder à l'acquisition en utilisant un logiciel/matériel approprié.</li> </ul>	<ul style="list-style-type: none"> <li>• Localiser les connecteurs JTAG.</li> <li>• Connecter un boîtier JTAG pour récupérer les données.</li> </ul>	<ul style="list-style-type: none"> <li>• Localiser les points de raccordement ISP.</li> <li>• Procéder à l'acquisition des données.</li> </ul>	<ul style="list-style-type: none"> <li>• Localiser la puce mémoire.</li> <li>• La retirer, la nettoyer et, si nécessaire, procéder à son rebillage.</li> <li>• Réaliser une image à l'aide d'un adaptateur et d'un outil de programmation appropriés.</li> </ul>

Figure 35 : Diagramme récapitulatif de l'examen d'une télécommande

### 5.2.6 Autres sources de preuves

Un drone peut être associé à de nombreux types d'équipements (charges utiles, accessoires électroniques, lunettes immersives/de réalité virtuelle), ou avoir subi des aménagements ou des ajouts. L'enquêteur et l'analyste de criminalistique numérique doivent garder un esprit ouvert quant aux pièces à conviction pouvant être utiles ou nécessaires pour faire avancer le dossier.

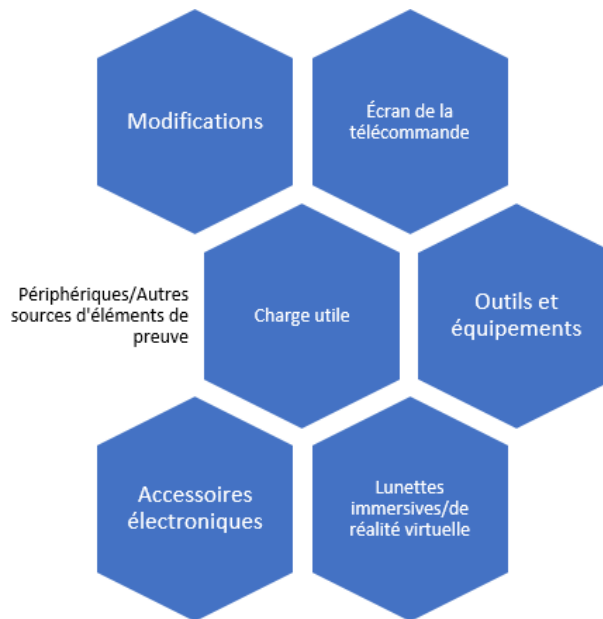


Figure 36 : Autres sources de preuves

On dit parfois que les données électroniques qui sont d'une importance primordiale pour l'enquête se trouvent sur un équipement associé comme un téléphone/ordinateur portable. Si un examen approfondi de cet équipement n'est pas possible, il convient d'essayer au moins un examen sommaire avec prise de notes.

### 5.3 Examen

L'examen des pièces à conviction doit, autant que possible, être évité. L'analyste doit toujours travailler sur une copie (c'est-à-dire un fichier image). Si ce n'est pas possible, la pièce à conviction doit être protégée contre l'écriture.

L'examen doit parfois avoir lieu dans un environnement isolé ou préparé à l'avance. C'est le cas par exemple pour effectuer une simulation sur une base de données ou un logiciel de jeu. L'analyste peut, pour ce faire, utiliser la technologie de la virtualisation et encapsuler les éléments du dossier dans un conteneur. Une fois l'examen terminé, il peut remettre la station de travail dans l'état où elle se trouvait auparavant en utilisant une image connue ou une fonctionnalité du système d'exploitation.

Pour en savoir plus sur les méthodes d'examen des éléments de preuve numériques, voir la section 5.2 des Principes directeurs d'INTERPOL liés aux laboratoires de criminalistique numérique.

### 5.4 Analyse

#### 5.4.1 Procédures d'analyse des traces numériques

De la même manière qu'un malfaiteur laisse des traces matérielles lorsqu'il quitte une scène de crime, un drone utilisé par un malfaiteur pour commettre une infraction conserve des traces et des indices des lieux visités et des actions effectuées, qui peuvent ensuite être récupérés (sur le drone ou des équipements associés).

Les données et les informations qui doivent être extraites d'un drone/d'une télécommande sont variables selon les cas.

### *a) Photos et vidéos*

Avant d'analyser des photos et des vidéos, l'analyste doit avoir une idée claire de ce que recherche le demandeur. L'enquêteur recherche-t-il des données multimédias créées sur l'appareil, ou des indices au sujet d'un acte criminel ? Passer en revue les photos et les vidéos stockées sur le drone permettra à l'analyste de comprendre l'usage qui est fait de l'engin ainsi que les lieux où il est utilisé.

Concernant les photos, leur analyse commence généralement par celle de leur signature. L'analyste peut ensuite opérer un tri parmi la galerie de photos en utilisant l'affichage en miniature.

S'agissant des vidéos, il est possible, avec certains logiciels, d'en extraire des images fixes (par exemple, un nombre Y d'images toutes les X secondes/minute). Ces images peuvent ensuite être visualisées comme des photos. Cela permet une prévisualisation beaucoup plus efficace des fichiers vidéo.

Dans les cas où il est important d'en savoir plus sur la localisation ou la réalisation des photos et des vidéos, on peut envisager d'extraire les métadonnées de ces fichiers. Les métadonnées fournissent des informations sur d'autres données : par exemple, les coordonnées GPS où la prise de vue a été réalisée, la date et l'heure de création, ainsi que l'appareil utilisé. Si les images ont été prises par le drone, elles comportent un géomarquage (il s'agit d'une fonction activée automatiquement par le drone, sauf si l'utilisateur a modifié la configuration).

Certaines pièces à conviction peuvent renfermer des milliers de photos et de vidéos, et il est donc impossible pour l'analyste de toutes les parcourir pour en sélectionner une en particulier. La meilleure façon de procéder est d'extraire l'ensemble des prises de vues et de les transmettre au demandeur. Par ailleurs, il peut y avoir sur le drone plusieurs copies d'une même photo ou vidéo se présentant sous un format miniature ou compressé.

La simple visualisation des prises de vues stockées sur le drone ne requiert aucune expertise en matière de criminalistique numérique et peut être effectuée par le demandeur. Une fois que ce dernier a repéré des prises de vues pertinentes, une analyse approfondie peut être réalisée par l'analyste en extrayant des données utiles comme des coordonnées GPS ou des informations sur la date de création ou de modification.

### *b) Journal de vol*

Le journal de vol d'un drone a, dans de nombreux cas, une valeur probante. Il contient généralement les traces numériques suivantes :

- Position GPS ;
- Date et heure ;
- Paramètres du drone (vitesse du rotor, altitude et direction) ;
- Données télématiques ;
- Codes d'erreur de diagnostic ;
- Fichiers journaux multimédias.

L'analyse de ces données peut fournir des informations importantes sur l'intention ou l'objectif de l'utilisateur du drone. Ainsi, le positionnement de l'engin à un certain endroit peut indiquer l'intention de son utilisateur de pénétrer dans un espace aérien protégé ou réglementé.

La plupart des logiciels d'analyse criminalistique permettent de passer au crible les journaux de vol. Toutefois, du fait des avancées technologiques et des mises à jour fréquentes de certains drones, certains de ces logiciels peuvent utiliser des bases de données non actualisées. Il est donc important que les analystes comprennent bien la structure sous-jacente de ces journaux. Dans la mesure où la plupart des drones utilisent la base de données SQLite ou des fichiers CSV, l'analyste peut décider d'analyser les traces numériques manuellement en les visualisant à l'aide du logiciel approprié.

Cela lui permet non seulement de ne pas dépendre d'un logiciel particulier, mais aussi d'effectuer une vérification croisée des résultats fournis par le logiciel.

#### *c) Applications/Logiciels*

Bien qu'il n'existe pas de procédures standard pour analyser toutes les traces numériques – compte tenu de leur diversité –, l'analyse est généralement réalisée en regroupant les informations provenant de sources sûres et fiables sur le logiciel ou l'application installé(e). Les résultats peuvent ensuite être vérifiés en effectuant une simulation ou en installant l'application sur un appareil de test et en réalisant des expérimentations pour comprendre le fonctionnement de l'application et la façon dont elle collecte des données. Cette façon de procéder permet en outre à l'analyste de mieux comprendre les droits d'utilisation de l'application et de savoir s'il est nécessaire de s'enregistrer.

#### *d) Activité de l'utilisateur*

Le système d'exploitation du drone enregistre l'activité de l'utilisateur à différents moments. Voici des exemples :

- Heures de mise en marche et d'arrêt du drone ;
- Configuration du drone ;
- Utilisation de l'appareil ;
- Comptes/identifiants de l'utilisateur ;
- Connexions wifi/de l'appareil ;
- Journaux télématiques.

L'analyse de cette activité permet de mieux comprendre le comportement de l'utilisateur, voire de prouver ce qu'il a fait. Selon le système d'exploitation, ces traces numériques sont stockées à différents endroits et dans différents fichiers.

#### *e) Espace non alloué*

Les zones non allouées peuvent contenir des traces de tous les types de preuve évoqués plus haut. La recherche et l'extraction de certains types de fichiers dans des espaces non alloués peuvent être effectuées automatiquement par un logiciel de reconstitution de fichiers. L'analyste doit toutefois préciser les types de fichiers recherchés car l'opération prend beaucoup de temps. L'opération de reconstitution ne fonctionne pas bien sur des fichiers fragmentés. La plupart du temps, les données se trouvant dans un espace non alloué sont impossibles à associer à un utilisateur, des informations horaires, ou même un emplacement dans une arborescence de dossiers.

#### *f) Stockage à distance et sur le nuage*

Lorsque l'analyste découvre sur un drone des traces de services infonuagiques, cela peut vouloir dire que :

- Les données sont stockées localement sur le drone et à distance sur le nuage ; ou
- Les données sont stockées intégralement sur le nuage. Le drone n'en contient aucune.



En fait, les données qui sont stockées à distance peuvent l'être sur plusieurs serveurs infonuagiques. La plupart du temps, le fournisseur de services infonuagiques lui-même ne sait pas sur quel serveur, centre de données ou pays sont stockées certaines données.

Bien qu'il soit techniquement facile de réaliser une copie numérique de la machine virtuelle qui se trouve sur le nuage pour y effectuer une expertise scientifique, sur le plan juridique, certains aspects sont à prendre en considération. Selon la législation applicable, le repérage des données et l'obtention d'une autorisation pour les intercepter peuvent être problématiques. Il peut aussi être difficile de s'assurer que les données sont acquises dans le respect des procédures en vigueur dans le pays demandeur.

Un autre inconvénient est qu'il risque d'y avoir très peu de données à extraire. Par exemple, si un malfaiteur a créé une machine virtuelle temporaire pour commettre des infractions et l'a ensuite supprimée, il n'y aura aucune preuve à récupérer.

La possibilité d'acquérir et d'analyser des données stockées à distance dépend du pays concerné et de sa législation. Dans certains pays, par exemple, l'analyste peut être autorisé à se connecter au serveur distant à l'aide des identifiants de l'utilisateur retrouvés sur le drone pour acquérir les données. D'autres pays n'autorisent pas l'acquisition des données. On peut alors passer par les canaux officiels pour solliciter la préservation et l'acquisition des données auprès du fournisseur des services.

## 5.5 Présentation

La phase de présentation consiste à regrouper les résultats de l'analyse de façon présentable et compréhensible pour les parties prenantes. Lorsque l'analyse est terminée, l'analyste établit un rapport présentant les constats et les résultats. Il doit, pour cela, illustrer et traduire des questions techniques complexes par des faits que les juges, procureurs et autres parties peuvent aisément comprendre. Il peut aussi avoir à interpréter ces faits et à donner son avis sur leur signification. Dans les cas où l'analyste a un grand nombre de pièces à conviction à analyser, il sera difficile pour lui de présenter les résultats aux enquêteurs. Il est alors recommandé d'utiliser un logiciel d'analyse pour faciliter la mise en correspondance de l'analyse des pièces à conviction avec d'autres données résultant de l'enquête. Ce type d'outil peut aussi servir à indexer et explorer toutes les pièces à conviction, de manière à fournir aux enquêteurs une vision d'ensemble de l'affaire.

### 5.5.1 Recevabilité des preuves électroniques

Les critères de recevabilité des preuves électroniques peuvent varier d'un pays à l'autre. En règle générale, les critères à prendre en considération avant de présenter des preuves devant un tribunal sont les suivants :

Critères généraux de recevabilité des preuves électroniques	
<b>Authenticité</b>	Les preuves doivent établir les faits de manière incontestable, et être conformes à leur état d'origine.
<b>Exhaustivité</b>	L'analyse des preuves, ou l'expression d'un avis les concernant, doit permettre de reconstituer tout ce qui s'est passé, et ne pas avoir à être adaptée pour correspondre à une vision plus favorable ou plus subjective.
<b>Fiabilité</b>	Rien dans la façon dont les preuves ont été recueillies puis analysées ne doit semer le doute quant à leur authenticité ou véracité.

Critères généraux de recevabilité des preuves électroniques	
<b>Force de conviction</b>	Les preuves doivent attester de façon convaincante des faits qu'elles représentent et être capables de convaincre les parties prenantes de la vérité qu'elles portent devant le tribunal.
<b>Proportionnalité</b>	Les méthodes employées pour recueillir les preuves doivent être justes et proportionnées aux intérêts de la justice : l'atteinte causée aux droits de quelque partie que ce soit (c'est-à-dire le niveau d'intrusion ou de contrainte) ne doit pas excéder la valeur probante des preuves (c'est-à-dire leur utilité au regard du droit).

Tableau 24 - Critères généraux de recevabilité des preuves électroniques

### 5.5.2 Rédaction du rapport

Le rapport d'expertise doit être rédigé dans un langage clair et compréhensible. Les résultats doivent être présentés de façon synthétique et apporter une réponse concise à la demande initiale.

Il est recommandé que les détails techniques soient fournis non pas dans le corps du document, mais dans des annexes. Le but est de faciliter la compréhension du rapport par le béotien.

L'auteur du rapport doit en outre s'abstenir d'affirmer des faits qui ne peuvent être prouvés : par exemple de dire « Le suspect a modifié le fichier A », alors qu'il conviendrait d'écrire « Le fichier A qui se trouve dans l'ordinateur B a été modifié ».

Les affaires sont parfois si complexes que l'analyste a du mal à présenter ses résultats dans un rapport. L'utilisation de supports et de représentations visuelles (animations, transparents, images et vidéos) est utile pour faciliter la compréhension.

### 5.5.3 Témoin expert

Dans certains systèmes judiciaires, l'envoi du rapport d'expertise au tribunal est suffisant ; dans d'autres, l'auteur du rapport doit obligatoirement assister à l'audience et présenter son témoignage d'expert.

Un témoin expert est une personne qui, en vertu de son niveau d'instruction, sa formation, ses compétences ou son expérience, possède une expertise et des connaissances spécialisées supérieures à un individu lambda. Ses connaissances sont telles que cette personne peut être contactée officiellement et dans un cadre légal pour donner son avis (dans le domaine scientifique, technique ou autre) au sujet d'une preuve ou d'un fait relevant de sa compétence, appelé avis d'expert.

Dans certains systèmes judiciaires, le statut d'expert est décidé au cas par cas par le juge, et l'expert ne jouit de ce statut que de manière ponctuelle ; dans d'autres, en revanche, ce statut est décidé par l'institution judiciaire, et l'expert intervient en tant que tel dans n'importe quelle affaire relevant de son domaine de compétence.

Les droits et les obligations du témoin expert diffèrent d'un pays à l'autre. Il est important pour les analystes de se familiariser avec la législation et les procédures judiciaires applicables, le rôle qu'ils ont à jouer ainsi que les droits et obligations qui y sont associés.

Pour en savoir plus sur l'assurance qualité et la recevabilité des preuves électroniques produites dans un laboratoire de criminalistique numérique, voir les sections 6.1 et 6.2 des Principes directeurs d'INTERPOL liés aux laboratoires de criminalistique numérique.

## 6. EXEMPLES DE DONNEES SE TROUVANT SUR UN DRONE







Les tableaux ci-dessous indiquent les emplacements courants des journaux de vol et fichiers multimédias sur certains modèles de drones connaissant actuellement un succès commercial.

### 6.1 Journaux de vol

Marque/Modèle du drone	Emplacement des données	Type de fichier	Nom par défaut
DJI Phantom 3	Mémoire interne	.dat	FLYXXX
DJI Phantom 4 Pro	Mémoire interne	.dat Deux fichiers journaux sont créés : PHARM.LOG et USER.LOG.	FLYXXX
DJI MAVIC 2	Mémoire eMMC	.dat	
YNEEX Q500 4K	Carte mémoire (pour une sauvegarde sur la télécommande)	.csv	Remote/RemoteGPS/Telemetry
Parrot ANAFI	Mémoire externe (ou iPhone pour une utilisation avec la télécommande)	.bin (.json)	Log.bin (XXDate&TlmeXX.json)

Tableau 25 - Emplacements des journaux de vol sur certains drones courants

### 6.2 Fichiers multimédias

Marque/Modèle du drone	Emplacement des données	Chemin du fichier	Type de fichier	Nom par défaut
 <b>DJI Phantom 3</b>				
 Photos	Mémoire externe	\DCIM\	.jpg/.dng	FLYXXX
 Vidéos	Mémoire externe	\DJI\dji.pilot\DJI_REC ORD\	.mp4/.mov	FLYXXX
 <b>DJI Phantom 4</b>				
 Photos	Mémoire externe	\DCIM\	.jpg/.dng	FLYXXX
 Vidéos	Mémoire externe	\DCIM\	.mov/.mp4	FLYXXX










 <b>DJI MAVIC 2</b>				
	<b>Photos</b>	Mémoire eMMC/ Mémoire externe	\DCIM\	.jpg/.dng FLYXXX
	<b>Vidéos</b>	Mémoire externe	\DCIM\	.mov/.mp4 FLYXXX
 <b>YUNEEC Q500 4K</b>				
	<b>Photos</b>	Mémoire de l'appareil photo	\DCIM\	.jpg/.dng
	<b>Vidéos</b>	Mémoire de la caméra	\DCIM\	.mp4
 <b>Parrot ANAFI</b>				
	<b>Photos</b>	Mémoire externe	\DCIM\100ME DIA	.jpg/.dng
	<b>Vidéos</b>	Mémoire externe	\DCIM\100ME DIA	.mp4
<p><b>* D'autres fichiers peuvent être enregistrés au format AVC sur la carte mémoire Micro SD de la télécommande, dans le répertoire \FPV-Video\Local\</b></p>				

Tableau 26 - Emplacements des fichiers multimédias sur certains drones courants

### 6.3 Applications mobiles associées

La majorité des drones utilisent des applications mobiles associées, que ce soit pour le pilotage, le visionnage des prises de vues ou l'affichage de la localisation de l'engin sur une carte. Ces applications requièrent généralement un compte de messagerie en cours de validité pour pouvoir y accéder, mais certaines sont également accessibles à l'aide d'un compte Facebook, Google, Apple ou Outlook. Toutes ces applications sont disponibles depuis la boutique Google Play Store et Apple Store, et nécessitent l'autorisation de l'utilisateur pour accéder à certaines fonctions du drone. Les tableaux ci-après donnent un aperçu des applications mobiles associées aux drones DJI, Parrot et Yuneec.

L'analyste de criminalistique numérique doit savoir qu'un drone peut être commandé ou suivi à l'aide d'une application tierce. Il doit donc, lorsqu'il examine le téléphone/l'ordinateur portable ou la tablette associé au drone, vérifier les fonctionnalités des applications qui y sont installées pour s'assurer qu'aucune d'elles n'est associée au drone analysé. L'analyse d'une application peut en outre faire apparaître des informations se rapportant à d'autres drones enregistrés.

Pour des conseils sur l'analyse criminalistique numérique des téléphones portables, se reporter aux Principes directeurs d'INTERPOL liés aux laboratoires de criminalistique numérique.

### 6.3.1 Application mobile associée aux drones DJI

Tous les drones DJI sont associés à des applications mobiles. L'application la plus utilisée est DJI Go 4.




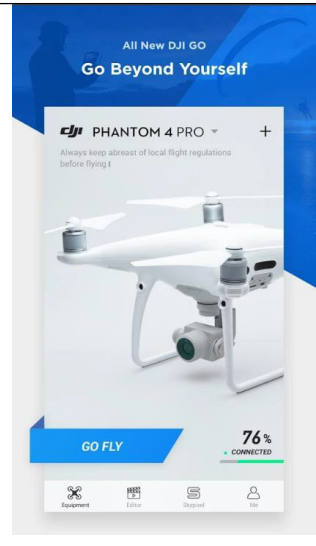
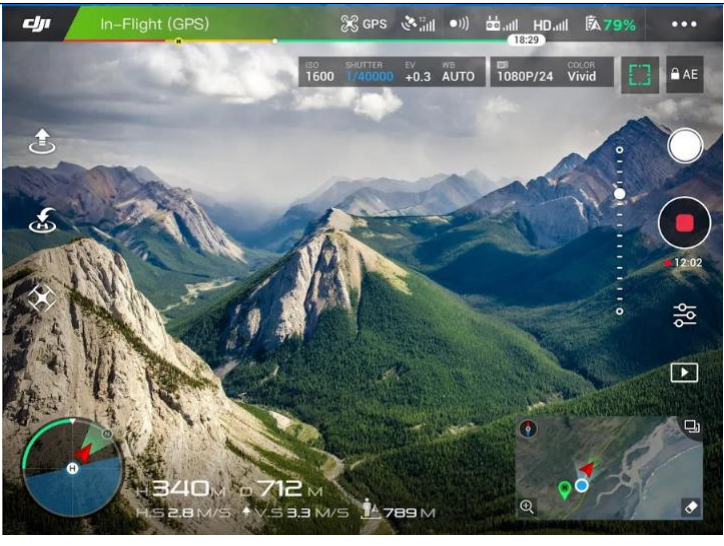
<b>Nom de l'application</b>	DJI Go 4
<b>Icône de l'application</b>	
<b>Éditeur</b>	DJI Technology
<b>Systèmes d'exploitation compatibles</b>	 iOS,  Android
<b>Description de l'éditeur</b>	
<p>Capturez le monde depuis le ciel. DJI GO 4.0 a été optimisée pour fonctionner avec tous les produits DJI les plus récents, tels que Phantom 4, Mavic Pro, Phantom 4 Pro et Inspire 2. L'application permet la transmission des images en temps quasi réel, le réglage des paramètres de prise de vue, ainsi que l'édition et le partage des vues aériennes.</p>	
<b>Caractéristiques :</b>	
<ul style="list-style-type: none"> <li>• Page d'accueil et interface utilisateur complètement relookées.</li> <li>• Transmission des images haute définition en temps quasi réel.</li> <li>• Réglage des paramètres de prise de vue.</li> <li>• Nouvelle interface de lecture.</li> <li>• Nouvel outil d'édition avec interface utilisateur améliorée.</li> <li>• Ajout de modèles et de pistes audio dans l'outil d'édition.</li> <li>• Facilité de téléchargement, d'édition et de partage des vidéos.</li> <li>• Mode de diffusion en continu intégré.</li> <li>• Enregistrement des données de vol en temps quasi réel.</li> </ul>	
<b>Captures d'écran</b>	
Écran d'accueil de l'application	Paramètres de vol
	

Tableau 27 - Application mobile DJI Go 4

### 6.3.2 Application mobile associée aux drones Parrot

<b>Nom de l'application</b>	FreeFlight Pro
<b>Icône de l'application</b>	
<b>Éditeur</b>	Parrot SA
<b>Systemes d'exploitation compatibles</b>	 iOS,  Android
<b>Description de l'éditeur</b>	<p>L'application officielle de pilotage pour les drones Parrot.</p> <p><b>PILOTEZ VOTRE DRONE À L'AIDE D'UN SMARTPHONE OU D'UNE TABLETTE.</b></p> <p>Téléchargez gratuitement FreeFlight Pro, l'application mobile qui vous permet d'avoir accès à des paramètres de vol avancés et de piloter votre drone Parrot Bebop, Bebop 2 ou Disco.</p> <p>Pour piloter ANAFI, veuillez utiliser la nouvelle application Freeflight 6. À noter que l'application Freeflight 6 ne peut pas être utilisée avec les drones de la gamme Parrot Bebop 2 et Parrot Disco.</p> <p><b>UN PILOTAGE INTUITIF</b></p> <p>Les commandes tactiles de FreeFlight Pro font du pilotage des drones Parrot un jeu d'enfant, que ce soit pour les débutants ou les pilotes plus aguerris. L'interface de l'application peut être personnalisée pour répondre au niveau de compétence de chacun. Si vous recherchez une expérience de pilotage plus poussée, connectez votre smartphone ou votre tablette à Parrot Skycontroller 2.</p>



### UN VOL EN IMMERSION

Montez à bord en chaussant les nouvelles lunettes immersives Parrot Cockpitglasses ! L'application FreeFlight Pro propose désormais un mode de pilotage en immersion qui, associé aux lunettes Cockpitglasses, vous procurera d'intenses frissons et d'extraordinaires sensations. Pour cela, il suffit d'insérer votre smartphone à l'intérieur des lunettes, de décoller et de vous laisser porter par la magie du vol. Lorsque le mode immersif est activé, les données télémétriques du vol s'affichent en direct sur votre écran afin de vous garantir un vol réussi.

### DES PHOTOS ET DES VIDÉOS DE QUALITÉ SUPÉRIEURE

FreeFlight Pro propose des paramètres de prises de vues avancés. Le mode photo vous permet de prendre des photos de grande qualité dans des formats professionnels (comme RAW/DNG). En mode vidéo, vous pouvez enregistrer des films de résolution Full HD 1080p à raison de 30 Mbits/s, et personnaliser la balance des blancs, l'exposition et la fréquence de rafraîchissement. Le mode échelonné permet des prises de vues à intervalles réguliers pour obtenir des vidéos en accéléré à couper le souffle. Enfin, profitez de la diffusion en temps réel des vidéos sur votre smartphone/tablette pendant le vol.

### PARROT CLOUD

En devenant membre de Parrot Cloud, vous pouvez garder une trace de toutes vos aventures et entrer en contact avec d'autres pilotes de drone. Partagez vos photos, vidéos et sessions de données avec d'autres pilotes, et transférez-les instantanément sur YouTube, Google Photos ou Twitter. En plus, toutes vos données partagées sont sauvegardées gratuitement sur Parrot Cloud.

### FLIGHT PLAN (disponible à l'achat sur l'application)

Avec Flight Plan (disponible à l'achat sur l'application), préparez des plans de vol à l'avance depuis votre smartphone ou votre tablette. Définissez des parcours de vol personnalisés en sélectionnant sur l'écran des points de passage. Puis faites décoller votre drone et laissez-le faire ! Enregistrez des vidéos époustouflantes grâce à ce mode intelligent, qui vous permet notamment de définir des points d'intérêt permettant de focaliser la séance de vol autour de certains objets.

### FIGURES ACROBATIQUES, LOOPINGS ET VIRAGES

L'application FreeFlight Pro inclut également des fonctions amusantes accessibles à l'aide d'une seule touche. Il vous suffit d'activer un bouton sur l'écran d'accueil pour faire virer, basculer et partir en looping votre drone Bebop.

Pour d'autres conseils et astuces de pilotage, et pour des tutoriels utiles sur la création de vidéos, visitez préalablement le site Parrot.com. Bon vol !


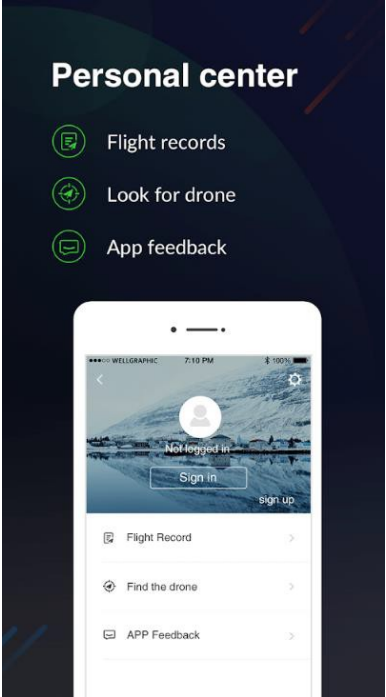
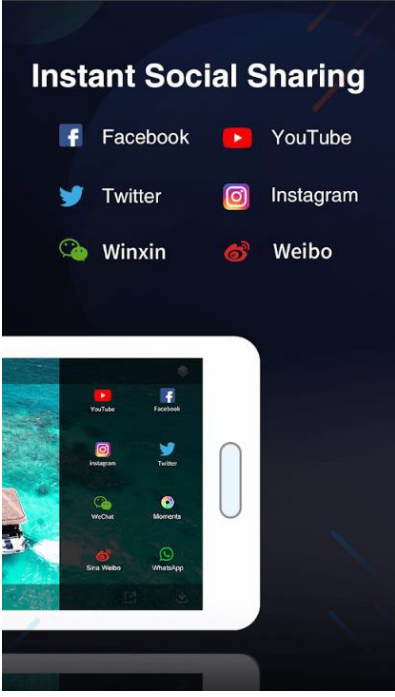
### Captures d'écran

	
Compatibilité de l'application	Utilisation de l'application comme contrôleur de vol

	
<p>Vue de l'application dans les lunettes Cockpitglasses</p>	

Tableau 28 - Aperçu de l'application mobile Parrot Freeflight

### 6.3.3 Application mobile associée aux drones Yuneec

<p><b>Nom de l'application</b></p>	<p>Yuneec Pilot</p>
<p><b> Icône de l'application</b></p>	
<p><b>Éditeur</b></p>	<p><a href="#">Yuneec International Co., Ltd</a></p>
<p><b>Systèmes d'exploitation compatibles</b></p>	<p>iOS, Android</p>
<p><b>Description de l'éditeur</b></p> <p>L'application Yuneec Pilot a été développée spécialement pour le drone de voyage Mantis Q. Compact et robuste, cet appareil vous permet de capturer des moments inoubliables en réalisant des photos uniques et des vidéos 4K. Grâce à son innovante commande vocale, son mode Sport en accéléré, sa longue autonomie de vol, ses modes de vol automatiques, sa reconnaissance commode des visages et sa fonction intégrée de partage sur les réseaux sociaux, Mantis Q vous garantit de passer d'excellents moments. Conçu pour être un compagnon de voyage facile à vivre pouvant être emporté n'importe où, ce drone est idéal pour les amoureux de la vie en plein air, les fans de gadgets et les amateurs de sensations fortes.</p>	
<p><b>Captures d'écran</b></p>	
	

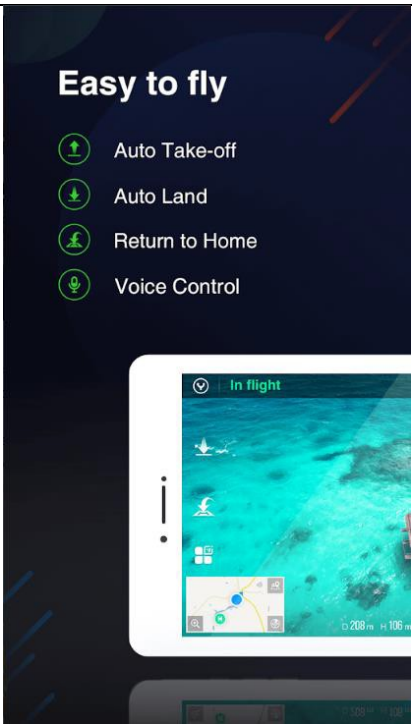
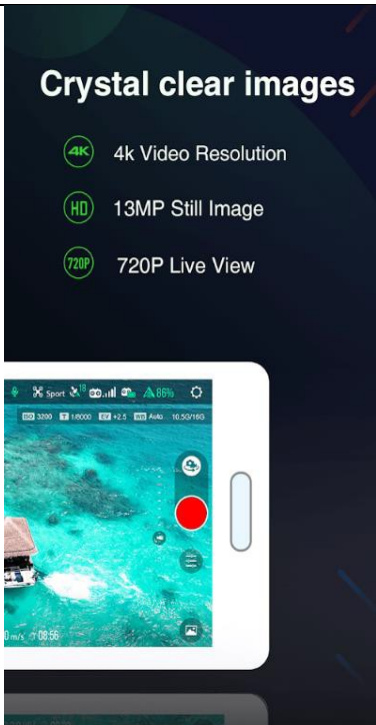
Écran de connexion au compte utilisateur	Fonction intégrée de partage sur les médias sociaux
	
Fonctionnalités de l'application	Fonctionnalités de l'application

Tableau 29 - Aperçu de l'application mobile Yuneec Pilot

### 6.3.4 Application mobile associée à une caméra de drone Yuneec

<b>Nom de l'application</b>	CG03
<b>Icône de l'application</b>	
<b>Éditeur</b>	Yuneec International Co., Ltd
<b>Systemes d'exploitation compatibles</b>	iOS, Android
<b>Description de l'éditeur</b> <p>CGO est un poste de contrôle au sol pour les appareils fonctionnant sous Android. L'application permet notamment de régler l'exposition, la sensibilité, la balance des blancs, la vitesse d'obturation, etc. Son développement étant en cours, en cas d'interrogation, n'hésitez pas à visiter notre site Web à l'adresse : <a href="http://www.yuneec.com">http://www.yuneec.com</a>.</p>	

### Captures d'écran



### Écran principal de l'application



### Écran des paramètres vidéo

Tableau 30 - Aperçu de l'application mobile associée à une caméra de drone Yuneec

Yuneec utilise également le système Android sur l'écran de ses télécommandes.



Figure 37 : Télécommande Yuneec



## 6.4 Emplacements de stockage sur les drones

Les données générées par les drones du fabricant Yuneec peuvent être stockées à trois endroits :

- le cardan de la caméra ;
- le drone ;
- la télécommande.



Figure 38 : Emplacements de stockage des données sur le Typhoon Q500 4K de Yuneec

Dans l'exemple ci-dessus, une carte mémoire peut être insérée à l'intérieur du drone, du dispositif de prise de vues et de la télécommande. Il est donc important que l'analyste de criminalistique numérique inspecte de façon approfondie le drone et les équipements associés pour s'assurer que tous les emplacements de stockage ont été repérés et analysés, en fonction des besoins.

De même, si le drone est associé à un téléphone portable ou une tablette, il est possible que l'application parente installée sur cet équipement renferme des traces numériques.

## 7. OUTILS COURAMMENT UTILISES POUR L'ANALYSE CRIMINALISTIQUE DES DRONES

Le marché des outils de police scientifique se rapportant aux drones n'en est encore qu'à ses balbutiements, et une majorité des outils disponibles dans le commerce pour l'analyse des drones font partie d'un ensemble plus vaste d'outils relevant de l'examen des appareils mobiles et l'informatique légale. Les capacités de ces outils peuvent varier d'un mois à l'autre, aussi il est conseillé, avant de choisir l'un ou l'autre, de toujours consulter les fabricants, la liste des appareils pris en charge et les types de données qui peuvent en être extraites.

### 7.1 Cellebrite/MSAB XRY/Oxygen/CFID

- Ces outils permettent le montage et la reconstitution des données extraites des drones. Le nombre de drones pris en charge est limité, mais lorsqu'ils sont utilisés à bon escient, ces outils simplifient le traitement des données se trouvant sur les drones et les équipements associés. Il est conseillé d'utiliser au moins deux de ces outils afin de pouvoir vérifier les données une fois qu'elles ont été extraites.

## 7.2 CsvView et DatCon [<http://datfile.net/>]

- DatCon est un outil au code source ouvert capable de reconstituer et de convertir dans différents formats (comme .kml et .csv) des fichiers .dat créés par un drone DJI. Il peut aussi transférer certaines données dans d'autres fichiers journaux (comme le journal de configuration et celui des événements).
- CsvView est un outil similaire, du même développeur, qui peut être utilisé pour reconstituer des données de fichiers journaux. Malgré son nom, il n'est pas réservé à des fichiers CSV et peut prendre en charge des journaux .dat originaux. Bien que similaires, ces deux outils présentent des capacités et des fonctionnalités différentes.

## 7.3 DROP (*DRone Open source Parser*) [<https://github.com/unhcfreg/>]

- DROP est développé par Devon Clark, en collaboration avec le *Cyber Forensics Research & Education Group* de l'Université de New Haven. Cet outil au code source ouvert peut être utilisé pour reconstituer et convertir des journaux de vol provenant de drones DJI Phantom 3. Il inclut en outre une décomposition partielle de la structure de données des journaux, issue du travail d'ingénierie inverse de DatCon.

## 7.4 Google Earth Pro [<https://www.google.co.uk/earth/versions/#download-pro>]

- Cet outil de cartographie, qui est capable de transmettre des données en ligne, peut être utilisé pour visualiser les données extraites des journaux de vol. Il a été testé avec succès avec des fichiers CSV et KML.

## 7.5 ST2Dash et Dashware [<https://github.com/ajpierson/st2dash> ; <http://www.dashware.net/>]

- Capables de transmettre des données en ligne.
- ST2Dash est un outil au code source ouvert conçu pour convertir les fichiers journaux de la télécommande ST10+ et du drone Q500 dans un format exploitable par Dashware. La suite logicielle Dashware, en accès libre, permet d'incruster des données télémétriques sur des images vidéo. Lors des tests, elle s'est avérée inutilisable à des fins d'analyse criminalistique car la synchronisation des données a pris beaucoup de temps et n'a pas fourni plus d'informations que celles qui étaient déjà disponibles. Elle est cependant utile dans certains cas.

## 7.6 DJI Assistant

- Cet outil peut être utilisé pour acquérir des données stockées sur un drone DJI. Il peut également reconstituer des journaux de vol ayant été récupérés, et les convertir au format .csv.

## 7.7 FTK Imager

- Permet de créer des images de cartes mémoire en vue de les analyser. À noter qu'une protection en écriture doit être utilisée.

## 7.8 VLC Player

- Ce lecteur multimédia polyvalent prend en charge de nombreux formats vidéo et codecs. Il peut être utilisé pour visualiser les fichiers multimédias générés par le drone examiné.



- Dans la mesure où les cartes mémoire internes et externes peuvent se présenter sous le format FAT32 ou exFAT, elles peuvent être facilement analysées à l'aide de suites logicielles de police scientifique comme FTK et Autopsy.

## 8. RESSOURCES WEB UTILES

De nombreux sites Web portent ou mettent l'accent sur les drones et le processus d'analyse criminalistique y afférent. Des sites utiles permettant de mieux comprendre les enjeux et les défis des drones sont fournis ci-dessous.

**Drone Forensics** [<https://www.droneforensics.com/>]

Le programme Drone Forensics a pour but de repérer sur les drones à usage privé et professionnel les données relevant de la criminalistique numérique, afin d'aider les services chargés de l'application de la loi et l'administration dans leurs enquêtes. Il est géré par la société VTO Inc., Broomfield/Colorado, États-Unis.

**Forensic Focus** [<https://www.forensicfocus.com/>]

Ce site Web donne accès à des forums de discussion très fréquentés sur la criminalistique numérique et renseigne sur l'actualité récente dans le domaine.

**Article « RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H »**

(<https://www.mdpi.com/1424-8220/19/15/3246>)






L'article rend compte de l'analyse des images produites par des drones à l'aide du référentiel CFReDS (*Computer Forensics Reference Datasets*), et des résultats obtenus pour le véhicule aérien Typhoon H fabriqué par Yuneec, Inc. Il examine la disponibilité et l'utilité des preuves numériques, qui permettraient de faciliter la conduite des enquêtes et de construire un dossier probant.

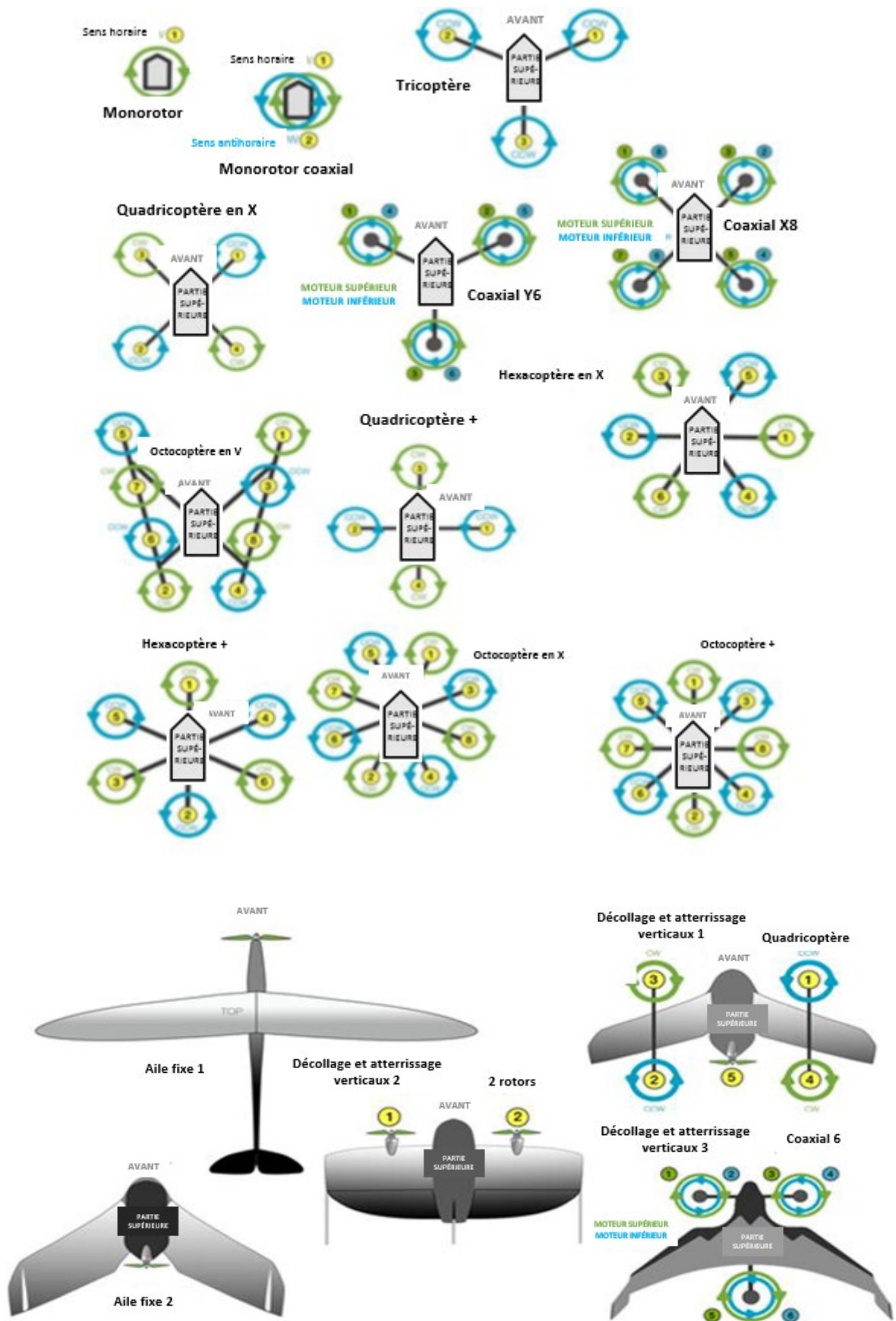
Autorités nationales de l'aviation civile (<https://www.OACI.int/pages/links.aspx>)

Ce répertoire fournit des informations détaillées sur toutes les autorités nationales de l'aviation, qu'il peut être utile de contacter en cas d'incident lié à un drone.



# Annexes

## Annexe A : Types de drones

Type de drone	Avantages	Inconvénients	Usages courants
<b>Multirotor</b> 	<ul style="list-style-type: none"> <li>● Accessibilité.</li> <li>● Facilité d'utilisation.</li> <li>● ADAV et vol stationnaire.</li> <li>● Bon contrôle du dispositif de prise de vues.</li> <li>● Peut fonctionner dans un espace confiné.</li> </ul>	<ul style="list-style-type: none"> <li>● Courte durée de vol.</li> <li>● Faible capacité de charge utile.</li> </ul>	<b>Photographies aériennes et inspections aériennes par vidéo.</b>
<b>Voilure fixe</b> 	<ul style="list-style-type: none"> <li>● Grande autonomie.</li> <li>● Grande couverture.</li> <li>● Grande vitesse de vol.</li> </ul>	<ul style="list-style-type: none"> <li>● Vaste espace nécessaire pour le décollage et l'atterrissage.</li> <li>● Pas d'ADAV ni de vol stationnaire.</li> <li>● Modèles non autonomes plus difficiles à faire voler et plus de formation requise.</li> <li>● Coût élevé.</li> </ul>	<b>Livraisons, cartographie aérienne et inspections de pipelines et de lignes électriques.</b>
<b>Monorotor</b> 	<ul style="list-style-type: none"> <li>● ADAV et vol stationnaire.</li> <li>● Grande autonomie (avec essence).</li> <li>● Capacité de transport d'une charge utile plus lourde.</li> </ul>	<ul style="list-style-type: none"> <li>● Plus dangereux.</li> <li>● Difficile à faire voler et plus de formation requise.</li> <li>● Coût élevé.</li> </ul>	<b>Téledétection aérienne par laser et numérisation.</b>
<b>Voilure fixe hybride</b> 	<ul style="list-style-type: none"> <li>● ADAV et grande autonomie.</li> </ul>	<ul style="list-style-type: none"> <li>● Pas très bon en vol stationnaire ou vers l'avant.</li> <li>● Toujours en cours de développement.</li> </ul>	<b>Livraisons.</b>
<b>Elios</b> 	<ul style="list-style-type: none"> <li>● Résiste aux collisions.</li> <li>● Conçu pour une utilisation à l'intérieur/ dans des espaces confinés.</li> <li>● Résiste à la poussière et aux éclaboussures.</li> </ul>	<ul style="list-style-type: none"> <li>● Coût élevé.</li> </ul>	<b>Accès à l'inaccessible et inspections des intérieurs/espaces confinés.</b>



### Types de batteries de drones

	
<p><b>Batterie LiPo compacte</b></p>	<p><b>Drone à usage récréatif</b></p>

### Types de télécommandes

		
<p><b>Dédiée</b></p>	<p><b>Associée</b></p>	<p><b>Associée de niveau supérieur</b></p>

## Annexe B : Compte rendu d'incident lié à un drone par les premiers intervenants

### Actions des premiers intervenants

#### Enregistrer l'incident

Prendre des photos ou des vidéos de l'engin en vol et des environs (au-dessus d'une foule, d'une zone construite, etc.).

Le survol d'une zone réglementée ou d'interdiction de survol (aéroport, base militaire, centrale nucléaire, prison) ou de toute zone spécialement désignée constitue une menace pour la sécurité publique.

#### Identifier le pilote

Le pilote se trouve très certainement à un endroit où il a un point de vue privilégié, qui lui permet de contrôler le drone. Il a sans doute les deux mains sur la télécommande (qui peut être une radiocommande standard, un smartphone, une tablette, etc.) et est concentré sur le contrôle du drone : il a le regard tourné dans sa direction et change peu d'orientation. Le pilote peut être en position statique ou marcher lentement. Son attitude est probablement très différente de celle des personnes autour de lui.

#### Entrer en contact avec le pilote et lui poser les questions suivantes :

Que fait-il ?

Que filme-t-il ?

Possède-t-il un permis d'utilisation du drone ?

#### Déterminer la nature de l'infraction :

Exemples d'infractions :

Trouble à l'ordre public

Agression

Acte criminel

Acte terroriste

Obstruction

Si une infraction a, selon vous, été commise, emmenez le pilote hors de la zone où se trouve la foule.

<b>Enquête préliminaire</b>
Déterminer l'endroit d'où a décollé le drone et celui où il a atterri.
Sécuriser la scène afin que le drone ne fasse courir de danger à personne.
Accéder à la zone de l'incident et évaluer la cause pour laquelle le drone se trouve à cet endroit :
<b>Drone</b>
De quel type de drone s'agit-il (multiroteur ou voilure fixe) ?
S'est-il écrasé ou a-t-il atterri ?
Est-il toujours en marche ?
Comporte-t-il une charge utile ?
Y a-t-il un danger évident (par exemple, risque d'explosion, hélices en mouvement, charge utile non déterminée) ?
<b>Télécommande/Pilote</b>
Pouvez-vous identifier le pilote du drone ?
La télécommande communique-t-elle encore avec le drone ?
Le pilote respecte-t-il vos injonctions ?
Se montre-t-il coopératif ?
Quel est le motif de l'utilisation du drone ?



**Sécurisation de la scène**

<b>Date</b>		
<b>Heure</b>		
<b>Lieu</b>		
<b>Coordonnées GPS</b>	<b>Longitude</b>	<b>Latitude</b>
<b>Vérifier s'il y a des dégradations sur le drone ou des indices de collision dans la zone environnante.</b>		
<b>Notes</b>		

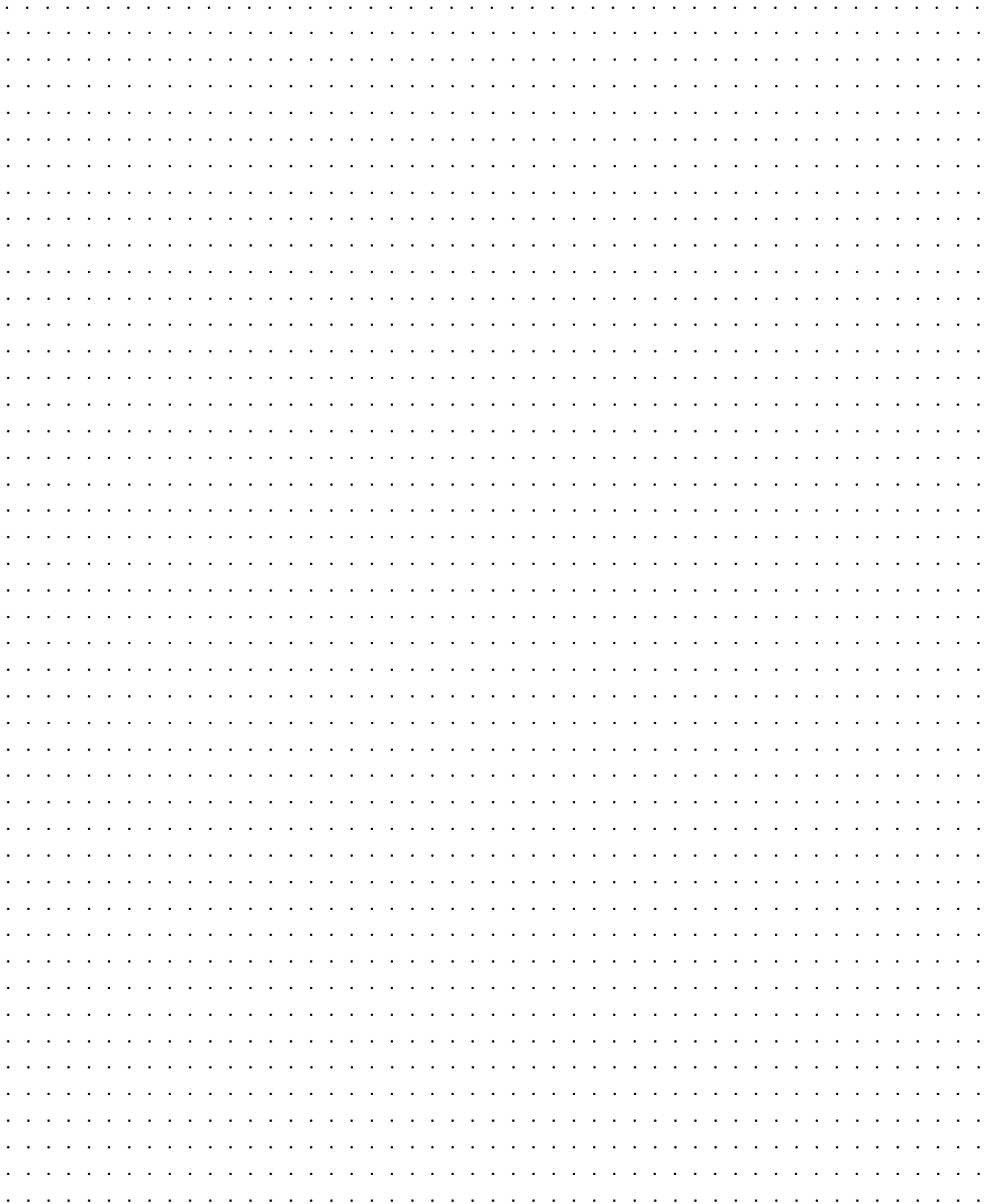
## Annexe C : Feuille d'enregistrement d'un incident lié à un drone

### Feuille d'enregistrement d'un incident lié à un drone

<b>Nom du policier présent</b>					
<b>Type de drone</b>					
<b>Multirotor</b>		<b>Voilure fixe</b>		<b>Monorotor</b>	
<b>Autre</b>					
<b>Fabricant</b>				<b>Modèle</b>	
<b>Le drone est-il en marche ?</b>	<b>Oui</b>		<b>Non</b>		
<b>En cas de mise hors tension du drone, préciser la méthode employée pour le faire :</b>					
<b>Bouton Arrêt</b>		<b>Retrait de la batterie</b>		<b>Autre</b>	
<b>Date</b>		<b>Heure</b>			
<b>Conditions météo (temps ensoleillé, pluvieux, nuageux, venteux)</b>					
<b>Notes</b>					

## Croquis de la scène

(Veuillez utiliser deux points de référence fixes et respecter l'échelle)



Des photos ont-elles été prises du drone et de la zone environnante ?			
Oui		Non	
L'exploitant du drone a-t-il été identifié ?			
Oui		Non	
Des équipements associés au drone ont-ils été mis en évidence et récupérés ?			
Oui		Non	
Équipements associés mis en évidence :			
Télécommande		Appareil mobile	
Batteries		Supports de stockage	
		Tablette	
		Autre	
Détails des autres équipements :			
Formulaire complété par		Coordonnées	
Signature			
Date		Heure	

## Annexe D : Compte rendu d'examen d'un drone

### Compte rendu d'examen d'un drone

#### Ce que doit savoir un laboratoire de criminalistique numérique pratiquant l'examen d'un drone

1. Un drone peut comporter à la fois une mémoire interne et un support de stockage amovible.
  - La mémoire interne peut contenir les journaux de vol et être accessible en démontant l'appareil.
  - Sur certains drones, l'accès à la mémoire interne peut se faire par un port USB. Il peut, dans certains cas, ne pas être possible de bloquer le processus d'écriture pour extraire les données de la mémoire interne.
2. Un drone stocke des données sur l'appareil lui-même et sur des périphériques qui lui sont connectés via un réseau (télécommande, ordinateur/téléphone portable, tablette, etc.)
  - Respecter les procédures d'acquisition de données applicables aux périphériques externes.
  - Utiliser les procédures de base de la criminalistique numérique pour extraire les données des périphériques externes.
3. Appliquer les procédures d'isolement réseau lors de l'examen d'un drone ou des appareils qui lui sont connectés.
4. Si le drone ne comporte ni mémoire interne, ni support de stockage amovible, il peut être nécessaire d'accéder à la mémoire flash se trouvant à l'intérieur de l'appareil.

**Premiers éléments de preuve/Détails sur l'affaire**








Nom/Identifiant de l'enquêteur	
Numéro de référence de l'affaire	
Service chargé de l'enquête	
<b>Stratégie de l'examen criminalistique</b>	
<b>(Expliquer brièvement tous les tests qui seront effectués sur les éléments de preuve reçus par le laboratoire).</b>	
<small>*Il s'agit juste d'une vue d'ensemble des travaux prévus, et non d'une description de ceux qui sont effectivement réalisés.</small>	



## Examen initial/Description physique de la pièce à conviction

Quel est l'appareil examiné ?			
<input type="radio"/> Drone	<input type="radio"/> Télécommande	<input type="radio"/> Téléphone	<input type="radio"/> Ordinateur/Autre
Si « Autre », préciser.			
Les éléments de preuve humides ont-ils tous été relevés (ADN, empreintes digitales, risque biologique, etc.) ?	<input type="radio"/> <b>OUI</b>	<input type="radio"/> <b>NON</b>	<input type="radio"/> <b>Non applicable</b>
Dans quel état se trouve la pièce à conviction examinée ?	<input type="radio"/> <b>Endommagée</b>	<input type="radio"/> <b>Modifiée</b>	<input type="radio"/> <b>Aucun dommage observé</b>
Si la pièce à conviction est endommagée ou modifiée, la décrire.			
Des photos de la pièce à conviction ont-elles été prises ?	<input type="radio"/> <b>OUI</b>	<input type="radio"/> <b>NON</b>	<input type="radio"/> <b>Non applicable</b>
Notes de l'analyste			
(Ajouter ici toute autre information)			

Notes relatives à l'examen d'un drone

<p>Fabricant</p>			
<p>Type de drone (cocher l'image appropriée)</p>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
	 <input type="checkbox"/>	<p>Autre – Ajouter un dessin</p>	
<p>Modèle</p>			
<p>Couleur</p>			
<p>Numéro de série/référence</p>			

	Préciser son emplacement (par exemple : dans la caméra, le drone, l'écran, autre) :	
Y a-t-il des supports de stockage amovibles (par exemple : carte mémoire, lecteur USB disque dur) ?	Type de support amovible (par exemple : Micro SD, carte mémoire, autre) :	
	Capacité de la carte mémoire :	
	Marque/Numéro de série :	
<p>Le drone comporte-t-il d'autres composants avec des étiquettes/numéros de série imprimés (en faire la liste en indiquant leurs numéros de série/référence) ?</p>		

Des photos des composants amovibles ont-elles été prises ?	<input type="checkbox"/> Oui	<input type="checkbox"/> Non	<input type="checkbox"/> Non applicable
	Préciser son emplacement (par exemple : dans la caméra, le drone, l'écran, autre) :		
Y a-t-il des supports de stockage amovibles (par exemple : carte mémoire, lecteur USB disque dur) ?	Type de support amovible (par exemple : Micro SD, carte mémoire, autre) :		
	Capacité de la carte mémoire :		
	Marque/Numéro de série :		
Le drone comporte-t-il d'autres composants avec des étiquettes/numéros de série imprimés (en faire la liste en indiquant leurs numéros de série/référence) ?			

Des photos des composants amovibles ont-elles été prises ?	<input type="checkbox"/> Oui	<input type="checkbox"/> Non	<input type="checkbox"/> Non applicable
--	------------------------------	------------------------------	---

## Notes de l'analyste

Quels types d'outils de police scientifique ont été utilisés pour l'acquisition de données ? (Indiquer le nom de l'outil et sa version.)		
Comment l'appareil examiné a-t-il été connecté à l'outil de police scientifique pour l'acquisition de données ?	Câble <input type="checkbox"/> Wifi <input type="checkbox"/>	Retrait de la puce <input type="checkbox"/> JTAG/ISP <input type="checkbox"/> Autre <input type="checkbox"/>
Quelle était la source d'acquisition des données (carte mémoire, mémoire interne, puce) ?		
Combien de temps a duré l'acquisition des données ?		
Notes sur l'examen (Indiquer les valeurs obtenues et tout comportement observé au cours de l'examen.)		
Date de fin de l'examen		
Heure de fin de l'examen		
Signature		

## Annexe E : Consignes de sécurité relatives aux batteries LiPo

### **Consignes de sécurité relatives aux batteries LiPo**

- **Les batteries en lithium doivent être manipulées avec soin car tout dommage ou court-circuit peut les faire s'enflammer.**
- **Lorsqu'elles ne sont pas utilisées ou en cours de chargement, les placer dans un sachet spécial et les tenir loin du feu.**
- **Si la batterie LiPo commence à augmenter de volume (à gonfler) ou si ses cellules ne se chargent pas toutes, il convient de la jeter.**
- **Avant de jeter la batterie, veiller à la décharger complètement en la connectant à une charge résistive (ampoule électrique ou chargeur/déchargeur).**
- **Il est recommandé de garder à proximité un seau métallique rempli de sable au cas où la batterie prendrait feu.**
- **NE PAS mettre de l'eau sur une batterie LiPo en feu, car le lithium utilise l'oxygène de l'eau et continue à brûler.**
- **Les batteries en lithium présentent souvent des dysfonctionnements au moment de la charge/décharge ou si on les fait tomber.**



## Annexe F : Liste de contrôle du kit d'intervention de base

Voici une liste des équipements de base qu'un laboratoire de criminalistique numérique doit avoir.  
La liste n'est cependant pas exhaustive et dépend de la nature des dossiers traités.

N°	Item	
1	Ordinateur portable	<input type="checkbox"/>
2	Logiciel de récupération et d'analyse des données de drones	<input type="checkbox"/>
3	Logiciel de récupération de données	<input type="checkbox"/>
4	Logiciel d'analyse d'appareils portables	<input type="checkbox"/>
5	Logiciel d'analyse et d'imagerie	<input type="checkbox"/>
6	Cage/Sacoche de Faraday	<input type="checkbox"/>
7	Appareil de prise de vues	<input type="checkbox"/>
8	Ruban de protection pour scènes de crime et matériel y afférent	<input type="checkbox"/>
9	Système de protection contre l'écriture	<input type="checkbox"/>
10	Supports de stockage vierges (pour y enregistrer à court et moyen termes les données extraites des preuves numériques) : <ul style="list-style-type: none"> <li>• Clé USB</li> <li>• Disque dur externe</li> <li>• Disque dur</li> </ul>	<input type="checkbox"/>
11	Kit d'outils électriques/électroniques	<input type="checkbox"/>
12	Rallonge électrique	<input type="checkbox"/>
13	Sac pour batterie LiPo	<input type="checkbox"/>

## Annexe G : Compétences de base des premiers intervenants et des professionnels de la criminalistique numérique

Voici une liste des compétences de base recommandées pour les premiers intervenants et les professionnels de la criminalistique numérique.

### 1. Objet

La présente annexe a pour objet de présenter les compétences de base des premiers intervenants – généralistes, techniques et avancés – et des professionnels de la criminalistique numérique dans le cadre d'un incident lié à un drone.

Niveau de compétence	
<b>ÉLÉMENTAIRE</b>	Premier intervenant généraliste
<b>INTERMÉDIAIRE</b>	Premier intervenant technique
<b>AVANCÉ</b>	Premier intervenant avancé
	Spécialiste de la criminalistique numérique appliquée aux drones

### 2. Champ d'application

Cette annexe s'adresse aux premiers intervenants qui découvrent un drone et les équipements qui y sont associés sur le lieu d'un incident. Les bonnes pratiques présentées ici sont préconisées en cas d'utilisation d'outils logiciels et matériels pour extraire les données du drone. Elles peuvent ne pas s'appliquer au personnel qui, au sein d'un laboratoire, utilise des outils de police scientifique pour récupérer ces données.

### 3. Définitions

L'analyse criminalistique des drones est l'utilisation de méthodes scientifiques pour récupérer les données stockées par un drone et les équipements qui y sont associés (tels qu'une télécommande ou des appareils mobiles) à des fins judiciaires.

### 4. Inconvénients

Les drones représentent un défi particulier pour les services chargés de l'application de la loi en raison des progrès rapides de la technologie. De nombreux modèles sont aujourd'hui utilisés et de nouvelles gammes sortent généralement sur le marché tous les trois à six mois. Un grand nombre de drones utilisent des systèmes d'exploitation fermés et des interfaces propriétaires, ce qui complique l'extraction d'éléments de preuve numériques par la police scientifique.

Les drones sont aussi associés à d'autres équipements comme une télécommande et un écran à affichage tête haute (qui peut être un téléphone portable ou une tablette). Une batterie et une carte mémoire peuvent aussi y être associées.

Les inconvénients sont les suivants :

Signaux entrants et sortants – Il convient d'essayer de bloquer les signaux entrants et sortants d'un drone et des équipements associés. Les méthodes courantes sont notamment l'utilisation d'appareils de blocage ou de brouillage des ondes radio. Outre le fait qu'il vide la batterie, le blocage des signaux radio peut coûter cher, n'est pas toujours efficace et risque d'entraîner l'altération des données du drone. Il permet toutefois de s'assurer que les données ne pourront pas être effacées à distance par l'exploitant du drone.

**Câbles** – Les câbles de transfert de données sont souvent particuliers à chaque drone. Ils sont souvent aussi spécifiques à chaque outil de police scientifique utilisé. Les normes de ces câbles sont diverses (par exemple : RJ-45, USB ou RS-232). Cela signifie qu'un grand nombre de câbles sont nécessaires pour procéder à l'analyse criminalistique d'un drone.

**Destruction des données** – Il existe des méthodes pour détruire les données d'un drone localement et à distance.

**Pilotes** – Des conflits peuvent survenir entre les pilotes du système d'exploitation, les pilotes propriétaires et ceux des revendeurs, ainsi qu'entre leurs versions respectives. Il peut être difficile de trouver des pilotes adaptés. Ceux-ci peuvent être fournis avec l'outil de police scientifique ou accessibles en téléchargement sur Internet. Si plusieurs logiciels sont installés sur la machine servant à l'analyse, les pilotes peuvent entrer en conflit pour obtenir le contrôle de la même ressource.

**Nature dynamique des données** – Lorsque le drone est en marche (allumé), les données qui s'y trouvent changent en permanence. Il n'existe pas de système standard de protection contre l'écriture pour les drones.

**Cryptage** – Les données peuvent être stockées dans un format crypté pour empêcher qu'elles soient analysées.

**Équipement** – L'équipement utilisé pour examiner un drone peut ne pas être le modèle le plus récent en raison de la nécessité pour le service chargé de l'application de la loi de vérifier le matériel, le microprogramme et/ou le logiciel.

**Analyse sur le terrain** – Les premiers intervenants doivent être conscients des risques associés à l'examen sommaire d'un drone. L'appareil doit être protégé avant de subir un examen approfondi.

**État des pièces à conviction** – Les outils vendus dans le commerce ne permettent pas nécessairement d'examiner des drones endommagés.

**Signature numérique** – La signature numérique de chacun des objets de données (graphiques, sons et vidéos) est souvent la même entre le poste de travail de la police scientifique et le drone. En revanche, du fait de la volatilité du système d'exploitation des drones, la signature des fichiers système n'est généralement pas la même, pour des raisons d'optimisation.

**Normes de l'industrie** – Les fabricants de drones n'utilisent pas tous les mêmes méthodes de stockage des données (certains utilisent des systèmes d'exploitation fermés et des connexions de données propriétaires).

**Baisse de puissance** – Lorsqu'ils sont déchargés ou éteints, il est fréquent que les drones perdent ou créent des données, ou enclenchent des mesures de sécurité.

**Cartes mémoire amovibles** – Examiner ces cartes à l'intérieur du drone présente des risques (cela empêche par exemple de récupérer toutes les données, dont celles effacées, et modifie l'horodatage).

**Formation** – La personne chargée d'extraire les données contenues sur un drone et les équipements associés doit avoir reçu une formation afin de préserver l'intégrité des données.

**Données effacées/se trouvant sur un espace non alloué** – Les outils utilisés pour l'analyse criminalistique des drones ne permettent souvent qu'une extraction logique des données. Or, les données effacées ne peuvent être récupérées qu'à l'aide d'une extraction physique.

**Équipement associé** – Un drone fonctionne à l'aide d'une télécommande et/ou d'un système de visualisation à distance, or cet équipement ne se trouve pas forcément à proximité du drone sur la scène de crime. Les batteries et les cartes mémoire associées au drone peuvent ne pas s'y trouver non plus.

## Annexe H : Compétences de base des premiers intervenants

### **Voici une liste des compétences de base recommandées pour les premiers intervenants.**

Les premiers intervenants sont des personnes chargées de recueillir le drone et de pratiquer sur lui un examen sommaire. On distingue trois catégories de premiers intervenants :

Premiers intervenants généralistes (niveau 1) : Ils recueillent et/ou examinent manuellement le drone et les équipements associés.

Premiers intervenants techniques (niveau 2) : Ils utilisent un outil ou un logiciel pour extraire les données du drone et des équipements associés. Les outils de base utilisés pour extraire/télécharger les données nécessitent une formation adaptée.

Premiers intervenants avancés (niveau 3) : Ils utilisent un outil ou un logiciel pour extraire les données du drone et des équipements associés. Les outils complexes utilisés pour extraire/télécharger les données nécessitent une formation adaptée.

Le domaine de l'analyse criminalistique des drones et des équipements associés ne cesse d'évoluer et présente des points communs avec l'informatique légale.

Les intervenants de niveau 3 doivent avoir une bonne connaissance globale de l'analyse criminalistique des appareils mobiles et doivent se tenir constamment informés en lisant des journaux spécialisés, en assistant à des cours, en intégrant des organisations professionnelles, en suivant une formation continue/en cours d'emploi et en acquérant de l'expérience pratique.

Ils doivent respecter l'ensemble des procédures et dispositions standard applicables, ainsi qu'un code de déontologie incluant la neutralité au cours du processus d'analyse scientifique.

Un premier intervenant peut se voir attribuer un dossier relevant d'un ou de plusieurs des niveaux présentés dans les annexes J et K. Il doit donc posséder le niveau de formation adéquat.

Niveaux d'analyse – Le niveau d'analyse dépend de la demande et des caractéristiques de l'enquête. Plus l'analyse est poussée et plus l'examen est approfondi.

## Annexe I : Compétences de base des premiers intervenants généralistes

**Voici une liste des compétences de base recommandées pour les premiers intervenants généralistes.**

1. Capacité à déterminer la configuration de base d'un drone.
  - a) Reconnaître les types de drones et les aéronefs non habités ;
  - b) Connaître les procédures d'arrêt qui conviennent pour le drone et les équipements associés.
2. Assurer la sécurité de la scène : comprendre comment sécuriser correctement la scène.
  - a) Scène de crime.
3. Interroger les personnes présentes (témoins, suspects).
4. Respecter les procédures de sécurité.
5. Savoir comment protéger les éléments de preuve : collecte, manipulation et emballage.
  - a) Prendre des photos de la scène de crime.
  - b) Étiqueter et numéroter les éléments de preuve.
  - c) Emballer correctement les éléments de preuve.
6. Préserver la chaîne de conservation des éléments de preuve.
7. Connaître le cadre juridique approprié.

## Annexe J : Compétences de base des premiers intervenants techniques

### **Voici une liste des compétences de base recommandées pour les premiers intervenants techniques.**

Les compétences ci-dessous correspondent aux exigences de base attendues de la part d'un premier intervenant technique qui examine manuellement un drone sur le terrain sans utiliser d'outil spécialisé.

- Ce type d'intervenant doit posséder toutes les compétences figurant à l'annexe I (« Compétences de base des premiers intervenants généralistes »), plus les suivantes :
- 1.** Connaître les procédures appropriées pour manipuler, étiqueter, préserver et saisir des éléments de preuve.
- 2.** Connaître les conséquences et les risques de la manipulation d'un drone.
- 3.** Savoir que le fait d'insérer des cartes mémoire dans différents appareils (ordinateur, appareil mobile ou drone) peut entraîner la modification des données.
- 4.** Savoir que le retrait et la remise en place de la batterie peut entraîner la réinitialisation du drone.
- 5.** Savoir quelle est l'autorité juridique compétente et connaître la jurisprudence.
- 6.** Savoir reconnaître les types de drones suivants : multirotors et à voilure fixe.
- 7.** Connaître l'importance de la description par écrit en bonne et due forme de la scène de crime.
- 8.** Connaître le processus de saisie d'un drone et des équipements associés.
- 9.** Connaître la nécessité et l'importance de vérifier les données extraites du drone et des équipements associés.
- 10.** Connaître les possibilités offertes par les équipements associés au drone (comme la télécommande et le téléphone portable utilisé pour visualiser les prises de vues).
- 11.** Savoir manipuler les batteries du drone de façon sécurisée afin de prévenir toute fuite ou explosion.
- 12.** Connaître les risques biologiques que peuvent présenter les drones ou équipements associés.
- 13.** Connaître les précautions d'usage concernant les éléments de preuve humides (empreintes digitales, ADN, etc.).



## Annexe K : Compétences de base des premiers intervenants avancés

**Voici une liste des compétences de base recommandées pour les premiers intervenants avancés.**

Les compétences ci-dessous correspondent aux exigences de base attendues de la part d'un premier intervenant technique qui utilise un outil pour examiner un drone et les équipements associés. Un exemple de ce type d'intervenant de niveau 3 est un policier patrouilleur ou un chargé de mission correctement formé qui utilise un logiciel ou du matériel pour extraire des données d'un drone et des équipements associés.

L'examen du système logique et du système de fichiers de ces appareils consiste par exemple à utiliser un logiciel ou un outil matériel pour en extraire des données accessibles par le système/l'utilisateur telles que : journaux de vol, positions d'origine, données télémétriques de vol, informations sur l'utilisateur, photos, vidéos, sons, données d'application et informations concernant l'appareil.

Ce type d'intervenant doit posséder toutes les compétences figurant à l'annexe I (« Compétences de base des premiers intervenants généralistes ») et à l'annexe J (« Compétences de base des premiers intervenants techniques »), plus les suivantes :

1. Connaître les acronymes importants utilisés pour décrire les composants des drones et leurs fonctions.
2. Savoir reconnaître les types de drones suivants : multirotors et à voilure fixe.
3. Savoir quelles informations peuvent être stockées sur un drone et les équipements associés.
4. Savoir quelles informations peuvent être stockées sur une carte mémoire.
5. Connaître les autres emplacements où peuvent être stockées des informations.
6. Connaître les aspects juridiques liés aux drones (par exemple : champ d'application d'un mandat, obtention d'une autorisation, jurisprudence, délivrance de permis et certifications requises).
7. Savoir isoler un drone de tout signal de commande, que ce soit en l'éteignant, en utilisant une protection contre les fréquences radio ou en désactivant toutes les communications radio.
8. Savoir expliquer les avantages et les inconvénients de la mise hors tension d'un drone.
9. Être capable de décrire les méthodes et les outils à utiliser pour examiner un drone et les équipements associés.
10. Connaître les fonctionnalités de l'outil utilisé, ses limites et la nécessité éventuelle de procéder à un examen complémentaire (à titre d'exemple, l'image logique des données peut ne pas permettre de retrouver les données qui ont été effacées sur le drone, sa télécommande et ses cartes mémoire).
11. Être conscient de la nécessité de procéder au test, à la maintenance et à la validation de l'outil utilisé pour l'examen.
12. Connaître les bonnes pratiques relatives à l'examen d'un drone.
13. Savoir que les données se trouvant sur les cartes mémoire peuvent ne pas être extraites à l'aide d'un logiciel ou d'un outil.
14. Être capable de justifier devant un tribunal les outils utilisés.

# Glossaires

---

## Présentation générale

- 1.1 Il faut savoir que la terminologie se rapportant aux opérations des aéronefs non habités ne cesse d'évoluer, et que le présent glossaire n'est par conséquent ni exhaustif, ni définitif. Il contient les définitions récentes de l'Organisation de l'aviation civile internationale (OACI), des termes « courants » considérés comme des alternatives acceptables et un certain nombre de termes « utilisés actuellement ». Même si ces derniers continueront à être reconnus, il est conseillé, pour des raisons d'homogénéité, d'utiliser les termes fournis dans les glossaires suivants.
- 1.2 Certains des termes des glossaires sont utilisés par les instances militaires, conformément aux publications réglementaires de l'autorité de l'aviation militaire du Royaume-Uni (*Military Aviation Authority Regulatory Publications*). Les termes en question (accompagnés d'un astérisque \*) ne s'appliquent pas nécessairement aux aéronefs non habités utilisés dans le domaine civil.

**NOTE :** Les termes « pilote » et « télépilote » sont de plus en plus usités à l'échelle mondiale (y compris par l'OACI) pour désigner la personne qui commande un aéronef non habité, et cette tendance se reflète dans le présent document. Au Royaume-Uni, de nombreuses obligations légales inscrites dans l'ordonnance sur la navigation aérienne de 2016 (« Air Navigation Order 2016 ») s'appliquent aux « pilotes ». Or, il s'agit ici du sens traditionnel du terme, c'est-à-dire des personnes qui se trouvent physiquement dans un aéronef et le font voler. Il n'existe à l'heure actuelle aucune disposition légale établissant les compétences nécessaires pour piloter un aéronef non habité ; ce travail reste à faire.

## Glossaire I : Acronymes utilisés dans l'aviation

### Acronymes couramment utilisés en liaison avec les drones

<b>BEAA</b>	Bureau d'enquêtes sur les accidents d'aviation
<b>ACAS</b>	Système anticollision embarqué
<b>AIP</b>	Publication d'information aéronautique
<b>ANSP</b>	Prestataire de services de navigation aérienne
<b>AOA</b>	Exploitant d'aéronefs*
<b>ATC</b>	Contrôle du trafic aérien
<b>ATM</b>	Gestion du trafic aérien
<b>ATS</b>	Services de la circulation aérienne
<b>ATSU</b>	Unité des services de la circulation aérienne
<b>BRS</b>	Ballistic Recovery Systems (entreprise)
<b>BVLOS</b>	Au-delà de la visibilité directe
<b>CFT</b>	Certificat d'essai de vol
<b>CPL</b>	Licence de pilote professionnel
<b>CRM</b>	Gestion des ressources de l'équipage
<b>C-UAV (C-UAS)</b>	Système de lutte contre les aéronefs sans pilote
<b>DA</b>	Zone de danger
<b>DAP</b>	Direction de la politique en matière d'espace aérien
<b>AESA</b>	Agence de l'Union européenne pour la sécurité aérienne
<b>ERF</b>	Restriction de vol d'urgence
<b>EVLOS</b>	Visibilité directe étendue
<b>FAA</b>	<i>Federal Aviation Administration</i>
<b>FIR</b>	Région d'information de vol
<b>FISO</b>	Responsable du service d'information de vol
<b>FMC</b>	Ordinateur de gestion de vol
<b>FOP</b>	Politique des opérations aériennes
<b>FRTOL</b>	<i>Flight Radio Telephony Operators' Licence</i>
<b>GCS</b>	Poste de contrôle au sol
<b>HALE</b>	Haute altitude et grande autonomie
<b>HMI</b>	Interface homme-machine

<b>OACI</b>	Organisation de l'aviation civile internationale
<b>IFR</b>	Règles de vol aux instruments
<b>JAA</b>	Autorités conjointes de l'aviation
<b>MAA</b>	<i>Military Aviation Authority</i> (Royaume-Uni)
<b>MALE</b>	Moyenne altitude et grande autonomie
<b>MOR</b>	Compte rendu obligatoire d'événements
<b>MRP</b>	Publications réglementaires de la MAA
<b>MTOM</b>	Masse maximale au décollage
<b>NOTAM</b>	Avis aux navigateurs aériens
<b>RA(T)</b>	Zone réglementée (temporairement)
<b>SER</b>	Surface équivalente radar
<b>RPA</b>	Aéronef télépiloté
<b>RPAS</b>	Système d'aéronef télépiloté
<b>RPAS Cdr</b>	Commandant de système d'aéronef télépiloté*
<b>RPS</b>	Poste de télépilotage
<b>RTF</b>	Radiotéléphonie
<b>SRG</b>	<i>Safety Regulation Group</i>
<b>SSR</b>	Radar secondaire de surveillance
<b>SUA</b>	Petit aéronef non habité
<b>SUAS</b>	Petit système d'aéronef non habité
<b>SUSA</b>	Petit aéronef de surveillance non habité
<b>TCAS</b>	Système anticollision
<b>TDA</b>	Zone de danger temporaire
<b>UAS</b>	Système d'aéronef non habité
<b>UAV</b>	Véhicule aérien sans pilote (terme utilisé actuellement)
<b>UIR</b>	Région supérieure d'information de vol
<b>VFR</b>	Règles de vol à vue
<b>VLOS</b>	Visibilité directe

Des explications de ces acronymes sont fournies dans les glossaires des pages suivantes.

## Glossaire II : Abréviations de termes techniques

---

### Abréviations courantes de termes techniques

<b>ACC</b>	Accéléromètre
<b>AUW</b>	Poids total en charge
<b>ARTF</b>	Presque prêt à voler
<b>AH</b>	Maintien de l'altitude
<b>mAh</b>	Milliampères-heures
<b>Rx</b>	Réception (par exemple d'un signal radio)
<b>Tx</b>	Émission (par exemple d'un signal radio)

## Glossaire III : Terminologie de la criminalistique numérique appliquée aux drones

### Termes courants de criminalistique numérique

A	
<b>Acquisition</b>	Voir « Image physique ».
<b>Copie d'archive</b>	Copie de données enregistrée sur un support de stockage à long terme, à partir de laquelle d'autres copies de travail peuvent être réalisées.
<b>Image d'archive</b>	Image enregistrée sur un support de stockage à long terme et correspondant à la reproduction au format binaire des données originales enregistrées sur un support de stockage à long terme.
<b>Authentification</b>	Processus consistant à prouver que les données correspondent exactement à ce qu'elles sont supposées être.
C	
<b>Capturer</b>	Processus consistant à enregistrer des données telles que des photos, des vidéos ou des informations de vol.
<b>Chaîne de conservation/ Continuité</b>	Enregistrement chronologique du déplacement, de l'emplacement et de la détention des éléments de preuve.
<b>Copie</b>	Reproduction fidèle d'informations.
D	
<b>Données</b>	Informations au format analogique ou numérique qui peuvent être transmises ou traitées.
<b>Analyse de données</b>	Évaluation des informations se trouvant sur des supports.
<b>Extraction de données</b>	Processus de repérage et de récupération d'informations qui ne sont pas toujours immédiatement apparentes.
<b>Souillure des données</b>	Altération des données par un système utilisé au cours d'un processus d'acquisition.
<b>Élément de preuve numérique/électronique</b>	Information stockée ou transmise au format binaire et présentant une valeur probante.

<b>Répertoire</b>	Liste de fichiers se trouvant sur un support. Peut aussi contenir des informations comme la taille et la date des fichiers.
<b>Télécharger/Exporter</b>	Processus de récupération de données numériques, de sons, de vidéos, de photos et de données transactionnelles. Peut avoir lieu sous un format natif ou propriétaire, ou sous un format ouvert.
<b>E</b>	
<b>Récupération de fichiers effacés</b>	Processus de restauration de fichiers qui avaient été supprimés.
<b>Extraire</b>	Procédé consistant à exporter des données depuis une source (par exemple : copier des données prévisualisées sous EnCas, ou dupliquer le contenu d'un téléphone portable). Voir Extraction de données.
<b>F</b>	
<b>Format de fichier</b>	Façon dont les données sont organisées à l'intérieur d'un fichier.
<b>Données résiduelles</b>	Données se trouvant entre la fin logique d'un fichier et la fin de la dernière unité de stockage de ce fichier. Dans le système de fichiers FAT, données se trouvant entre la fin logique d'un fichier et la fin d'un cluster.
<b>Expertise</b>	Utilisation ou application de connaissances scientifiques dans le cadre d'une question de droit, et plus particulièrement d'une enquête criminelle.
<b>Clonage numérique</b>	Processus de reproduction de données au format binaire entre un support physique et un autre.
<b>G</b>	
<b>Géomarquage</b>	Coordonnées de géopositionnement ajoutées aux fichiers sous forme de métadonnées.
<b>GPX</b>	Format de fichier permettant l'échange de données de géopositionnement. Subdivision du format XML permettant de disposer, dans les applications logicielles, d'un format commun pour les données GPS.
<b>H</b>	
<b>Signature numérique</b>	Ensemble de valeurs numériques générées par des fonctions de hachage, qui servent à vérifier l'intégrité d'éléments de preuve numériques et/ou à effectuer des comparaisons par rapport à des séries de valeurs connues afin de voir s'il y a eu des ajouts/suppressions.
<b>I</b>	
<b>Vérification d'intégrité</b>	Processus visant à confirmer que les données présentées sont complètes et n'ont subi aucune altération depuis leur acquisition.



L	
<b>Fichier journal</b>	Enregistrement des actions, événements et données connexes.
<b>Acquisition/Copie logique</b>	Reproduction fidèle des informations contenues sur une unité logique (volumé monté, lecteur, etc).
M	
<b>Support</b>	Dispositif pouvant accueillir des données.
<b>Métadonnées</b>	Données le plus souvent incorporées à un fichier, qui décrivent ce fichier ou le répertoire (notamment son emplacement, la date et l'heure, des informations concernant l'application et les autorisations).
<b>Appareil mobile</b>	Appareil portatif possédant une architecture système intégrée, un processeur, une mémoire interne et parfois des fonctionnalités de téléphonie.
<b>Analyse criminalistique d'un téléphone portable</b>	Utilisation de méthodes scientifiques pour récupérer des données sur un téléphone cellulaire dans un cadre légal.
<b>Éléments de preuve multimédias</b>	Supports analogiques ou numériques (comme des vidéos, des bandes son, des supports magnétiques et optiques) et/ou les informations qui s'y trouvent.
N	
<b>Format de fichier natif</b>	Forme originale d'un fichier. Un fichier créé dans une certaine application peut souvent être lu dans d'autres, mais le format natif reste celui qui a été donné par l'application dans laquelle le fichier a été créé. Dans la plupart des cas, les attributs d'un fichier (par exemple, les polices utilisées dans un document) ne peuvent être modifiés que dans l'application où le fichier a été créé.
P	
<b>Récupération de mot de passe</b>	Processus consistant à repérer et mettre en évidence une série de caractères servant à restreindre l'accès aux données.
<b>Circuit imprimé</b>	Carte utilisée dans le domaine électronique. Désigne la carte elle-même ou ses composants.
<b>Examen par les pairs</b>	Évaluation de rapports, notes, données, conclusions et autres documents réalisée par un second individu qualifié.
<b>Copie physique</b>	(c) Fidèle reproduction des informations se trouvant sur un support physique.
<b>Image physique/Acquisition</b>	(c) Reproduction au format binaire des données se trouvant sur un support.

<b>Pixel</b>	Élément le plus petit entrant dans la composition d'une image et pouvant subir un traitement individuel dans un système d'imagerie électronique [ <i>The Focal Encyclopedia of Photography</i> , 4 <sup>ème</sup> édition 2007].
<b>Lecture</b>	Visionnage et écoute d'un contenu ayant été enregistré à l'aide d'un caméscope, d'un magnétophone ou d'un autre appareil.
<b>Prévisualisation</b>	(c) Examen sommaire et rapide d'éléments afin d'évaluer la nécessité de les collecter et/ou de réaliser un examen plus approfondi.
<b>Image principale</b>	Image enregistrée pour la première fois sur un support et qui constitue un objet individuel doté de caractéristiques propres. Il s'agit par exemple d'une image numérique enregistrée sur une carte Flash, ou téléchargée d'Internet.
<b>Image traitée</b>	Image ayant subi un traitement (amélioration, restauration ou autre).
<b>Test d'aptitude</b>	<p>Test visant à évaluer les analystes, le personnel de soutien technique et la qualité du travail d'un organisme (<i>voir les quatre types de tests ci-dessous</i>).</p> <ol style="list-style-type: none"> <li>1. <b>À découvert</b> - Les analystes et le personnel de soutien technique savent qu'ils font l'objet d'un test.</li> <li>2. <b>À l'insu</b> - Les analystes et le personnel de soutien technique ignorent qu'ils font l'objet d'un test.</li> <li>3. <b>Interne</b> - Le test est réalisé par l'organisme lui-même.</li> <li>4. <b>Externe</b> - Le test est réalisé par un organisme tiers indépendant.</li> </ol>
<b>Format de fichier propriétaire</b>	Format de fichier spécifique à un fabricant ou à un produit.
<b>Q</b>	
<b>Assurance qualité</b>	Ensemble d'actions planifiées et systématiques visant à fournir une garantie suffisante que le produit ou le service fourni par un organisme/laboratoire satisfera à des exigences données en matière de qualité.
<b>R</b>	
<b>Reconstruction</b>	Processus de réparation d'un support endommagé afin de pouvoir y récupérer des données.
<b>Informations de référence</b>	Peuvent inclure : publications, documentation relative à du matériel ou un logiciel, jeux de hachage, en-têtes, etc.
<b>Fiabilité</b>	Degré selon lequel une information est jugée sûre.
<b>Reproductibilité</b>	Capacité pour un processus de donner les mêmes résultats à chaque occurrence.

<b>Résiduel(le)</b>	(c) Se dit d'une donnée se trouvant dans un espace de marge ou non alloué.  (a) Se dit d'un signal correspondant à la différence algébrique entre le signal d'entrée et les résultats de son filtrage [ <i>Diamond Cut Users Manual</i> ].
<b>Résolution</b>	Acte, processus ou capacité de distinction entre deux éléments ou résultats de stimuli différents mais adjacents, comme les détails d'une image ou des couleurs similaires [ <i>Encyclopedia of Photography</i> , 3ème édition].
<b>S</b>	
<b>Code source</b>	Liste d'instructions rédigées dans un langage de programmation pour concevoir un logiciel.
<b>Support de stockage</b>	Dispositif permettant de conserver des données.
<b>T</b>	
<b>Examen technique</b>	Évaluation de rapports, notes, données, conclusions et autres documents réalisée par un second individu qualifié.
<b>Reconstitution d'une séquence chronologique</b>	Processus consistant à relier des images, des sons ou d'autres données selon un ordre chronologique.
<b>Journal de suivi</b>	Liste complète de positions enregistrées par un système de géopositionnement.
<b>Examen sommaire</b>	Processus consistant à examiner brièvement des éléments afin de déterminer s'ils doivent être collectés et/ou analysés, et si oui, dans quel ordre.
<b>U</b>	
<b>Espace non alloué</b>	Zone de stockage de données disponible sur un ordinateur. Cette zone peut contenir des informations y ayant été préalablement stockées. Également appelé <i>Espace libre</i> .
<b>V</b>	
<b>Validation</b>	Ensemble d'expérimentations permettant d'établir l'efficacité et la fiabilité d'un outil, d'une technique ou d'une procédure, ou de confirmer une modification leur ayant été apportée.
<b>Test de validation</b>	Essai visant à déterminer si un outil, une technique ou une procédure fonctionne correctement et comme prévu.
<b>Vérification</b>	Processus visant à confirmer la conformité d'un élément avec l'original.  Confirmation qu'un outil, une technique ou une procédure fonctionne comme prévu.
<b>Vidéo</b>	Enregistrement au format électronique d'un enchaînement d'images représentant des scènes statiques ou en mouvement. Peut contenir des sons.

W	
<b>Point de passage</b>	Position stockée par un dispositif de géopositionnement suite à l'interaction de l'utilisateur.
<b>Exemplaire de travail</b>	Copie ou reproduction d'un enregistrement ou de données pouvant être utilisée ultérieurement à des fins de traitement et/ou d'analyse.
<b>Protection contre l'écriture</b>	Procédés matériels et/ou logiciels permettant d'empêcher la modification des données se trouvant sur un support.

Note : Les définitions proviennent du glossaire « Digital & Multimedia Evidence Glossary Version 3.0 » (23 juin 2016) du SWGDE (*Scientific Working Group on Digital Evidence*).

## Glossaire IV : Termes relatifs aux UAV

## Termes courants concernant les UAV

0-9	
<b>2,4 GHz</b>	Fréquence utilisée pour les communications numériques (étalement du spectre) des drones, y compris par les télécommandes, la technologie Bluetooth et certains appareils de vidéo-transmission. Cette bande n'est pas la même que l'ancienne bande de 72 Mhz qui est utilisée pour les communications analogiques. Pour éviter un conflit de fréquences, il est souvent conseillé d'utiliser des équipements radio de 72 Mhz avec des émetteurs vidéo de 2,4 GHz, ou des équipements radio de 2,4 GHz avec des émetteurs vidéo de 900 Mhz. 2,4 GHz se trouve généralement dans une bande de fréquences sans licence.
<b>Cartographie 3D</b>	Création de cartes 3D à l'aide d'un progiciel depuis un drone. Parce qu'il permet de cartographier rapidement et efficacement de vastes zones, ce progiciel est utile aux agriculteurs pour améliorer la rotation de leurs cultures, aux compagnies d'assurance pour évaluer des dommages sur des bâtiments sans faire courir de risques humains, aux compagnies forestières pour délimiter le couvert arboré, et aux architectes pour réaliser la topographie précise d'un site à des fins d'aménagement.
<b>5,8 GHz</b>	Fréquence couramment utilisée, la plupart du temps par les micro-ondes, la technologie Bluetooth, les drones, etc. Son utilisation pour un drone peut donc être perturbée par les interférences provenant d'autres appareils sans fil ou d'autres drones. 5,8 GHz se trouve généralement dans une bande de fréquences sans licence.
A	
<b>Accéléromètre</b>	Appareil mesurant les forces d'accélération dans une direction donnée. Il est utilisé pour stabiliser les quadricoptères, souvent lorsqu'il y a du vent.
<b>Mode ACRO</b>	Également appelé « mode RATE », il permet de contrôler la vitesse angulaire du drone à l'aide de la télécommande. Il est utilisé la plupart du temps lorsque l'on fait basculer ou tourner sur lui-même un drone.
<b>Vitesse ascendante</b>	Vitesse à laquelle le drone s'élève dans l'air. La vitesse ascendante du Wind 4, par exemple, est de 4 mètres par seconde.
<b>Mode ATTI</b>	Ou mode Attitude. C'est le mode dans lequel le drone maintient son altitude quelle que soit la pression barométrique. Sa position n'est pas stabilisée à l'aide du système GPS ou GLONASS. Cela signifie que si le drone est poussé par le vent, il ne gardera probablement pas la même position, et il faudra alors réajuster sa trajectoire.

<b>Aéronef (OACI)</b>	Engin pouvant se maintenir dans l'atmosphère grâce aux réactions de l'air autres que celles se produisant contre la surface de la Terre.
<b>Cellule</b>	Ensemble de la structure physique d'un UAV, nécessaire pour assurer un vol équilibré.
<b>Poids total en charge</b>	Poids total d'un aéronef avec sa batterie et d'autres pièces.
<b>Presque prêt à voler (ARTF)</b>	Autre acronyme utilisé : ARA. Le coffret du drone comprend tout ce qu'il faut, mais des opérations d'assemblage peuvent être nécessaires. Cela signifie généralement que le récepteur n'est pas fourni.
<b>Maintien de l'altitude (AH)</b>	Un altimètre barométrique est utilisé pour maintenir le drone à la même altitude.
<b>Auto-level</b>	Mode de vol permettant à l'aéronef de se maintenir à niveau, en utilisant l'accéléromètre et le gyroscope.
<b>Aéronef autonome</b>	Aéronef non habité ne permettant pas au pilote d'intervenir dans la gestion du vol. Il s'agit d'une sous-catégorie des aéronefs non habités.
<b>Vol autonome</b>	Vol guidé par les points de passage GPS.
<b>Fonctionnement autonome</b>	Fonctionnement d'un aéronef télépiloté sans que le pilote n'intervienne dans la gestion du vol.
<b>B</b>	
<b>Altimètre barométrique</b>	Capteur de mesure de l'altitude. Il utilise la pression barométrique – comme l'émetteur – et contrôle le drone/quadricoptère en vol depuis le sol.
<b>Batterie</b>	Plusieurs types de batteries sont utilisés sur les drones. Qu'elle soit amovible ou non, la batterie peut faire fonctionner le contrôleur de vol, le récepteur ou le matériel de vidéo-transmission.
<b>BeiDou</b>	Système chinois de navigation par satellite composé de deux constellations de satellites différentes.
<b>Liaison</b>	Procédure de mise en relation entre le drone et la télécommande.
<b>BNF (Bind aNd Fly)</b>	Les produits BNF contiennent tout ce qu'il faut pour utiliser un drone, sauf l'émetteur. L'utilisateur peut alors se servir de son propre émetteur et le relier au récepteur fourni avec le drone.

<b>Moteur sans balais</b>	Moteur constitué d'aimants permanents qui tournent autour d'une armature fixe, ce qui élimine les problèmes dus au passage du courant dans la partie en mouvement. Ce type de moteur est nettement plus efficient et durable que les moteurs à balais en raison de l'absence de frottements, qui permet de réduire le bruit et d'accroître la fiabilité.
<b>BVLoS (ou <i>Beyond the Visual Line of Sight</i>)</b>	Les vols de drone BVLOS sont effectués « au-delà de la visibilité directe » du pilote. Dans la plupart des pays, ces types de vols sont interdits ou soumis à autorisation. Selon la réglementation en vigueur au Royaume-Uni, les vols de drones doivent avoir lieu dans les limites de la visibilité directe ordinaire, c'est-à-dire jusqu'à 122 mètres de hauteur et 500 mètres dans chaque direction.
<b>C</b>	
<b>Centre de gravité</b>	Point d'équilibre moyen d'un drone.
<b>Canal</b>	Fréquence utilisée par un émetteur vidéo ou fonction de liaison entre le contrôleur-émetteur et le drone. Un canal peut par exemple être attribué pour contrôler la commande des gaz ou allumer/éteindre les feux de navigation. La plupart des drones utilisent au moins six canaux.
<b>Espace aérien contrôlé</b>	Espace aérien de dimensions définies à l'intérieur duquel le service du contrôle de la circulation aérienne est assuré pour les vols aux instruments et les vols à vue, selon la classification des espaces aériens.
<b>Zone de contrôle (CTR)</b>	Espace aérien contrôlé s'étendant verticalement de la surface jusqu'à une limite supérieure spécifiée.
<b>Télécommande</b>	Appareil portable utilisé par le pilote d'un drone pour en assurer le contrôle. Également appelé émetteur.
<b>Liaison de contrôle et de commande (C2) (OACI)</b>	Liaison de données entre l'aéronef télépiloté et le poste de télépilotage aux fins de la gestion du vol.
<b>C-UAV</b>	Technologie antidrones, également appelée C-UAS ou C-UAV. Désigne les systèmes utilisés pour détecter et/ou intercepter les aéronefs non habités. Voir aussi DTI.
<b>D</b>	
<b>Vitesse descendante</b>	Vitesse à laquelle un drone se dirige vers le sol. Elle est par exemple de trois mètres par seconde.



<b>Détection et évitement (OACI)</b>	Possibilité de voir, de prévoir ou de détecter les conflits de circulation ou tout autre danger et de prendre les mesures appropriées. Les fonctions de séparation en vol et d'évitement des collisions sont assurées, de la même manière que sur les aéronefs habités.
<b>DTI (Detect, Track and Identify)</b>	Méthode de détection, de suivi et d'identification en temps réel des objets mobiles (y compris les UAV) à l'aide d'un ou de plusieurs capteurs.
<b>DJI Aeroscope</b>	Technologie antidrone de DJI. En interceptant la liaison de communication entre un drone DJI et sa télécommande, Aeroscope est capable d'envoyer en temps réel des informations d'identification, notamment le numéro de série de l'UAV, son fabricant et son modèle, sa position, sa vitesse, son altitude et la localisation du poste de contrôle au sol.
<b>Drone</b>	Terme couramment employé pour désigner les véhicules aériens non habités, ou UAV. Il recouvre de nombreux types d'aéronefs différents, de tailles variées, utilisés à des fins très diverses, que ce soit par les forces armées ou par des amateurs effectuant des photos numériques à titre de loisir. Une autre appellation du drone est « aéronef télépiloté » (RPA).
<b>DSM / DSM2 / DSMX</b>	Technologie propriétaire de modulation numérique mise au point par Spektrum, fabricant de matériel de commande radio. Chaque émetteur possède un identifiant universel unique (GUID) auquel les récepteurs peuvent être liés, afin de prévenir les interférences avec tout autre système DSM de Spektrum situé à proximité. Les systèmes DSM utilisent la technologie d'étalement de spectre à séquence directe (DSSS).
<b>DSSS</b>	Le DSSS, ou étalement de spectre à séquence directe, est une technique de modulation. Comme pour d'autres technologies d'étalement de spectre, le signal émis occupe une plus grande bande de fréquences que le signal qui module la fréquence porteuse ou d'émission. L'expression « étalement de spectre » vient du fait que le signal de la porteuse occupe toute la bande (le spectre) de la fréquence d'émission d'un appareil.
<b>E</b>	
<b>Interférence électromagnétique</b>	Interférence électrique pouvant provenir de sources externes.
<b>Variateur de vitesse électronique</b>	Dispositif de contrôle du moteur d'un aéronef électrique, qui traduit les signaux provenant du contrôleur de vol pour les envoyer aux moteurs gérant la vitesse et le sens de rotation. L'appareil comprend aussi généralement un circuit d'élimination de batterie, qui alimente le système de commande radio et autres composants électroniques embarqués comme le système de pilote automatique.

<b>Mémoire morte programmable effaçable électriquement (EEPROM)</b>	Type de mémoire non volatile utilisée sur les ordinateurs et autres appareils électroniques pour stocker de petites quantités de données qui doivent être conservées une fois l'alimentation coupée (par exemple, des tables de référence/d'étalonnage statique). Contrairement à ce qui se passe pour la plupart des autres types de mémoire non volatile, chaque octet se trouvant dans une EEPROM classique peut être lu, effacé et écrasé.
<b>Gouverne de profondeur</b>	A pour corollaire le « tangage ». Voir la définition de ce terme.
<b>EVLOS</b>	Visibilité directe étendue. Cela équivaut à utiliser un drone au-delà des règles de base, le plus souvent en faisant appel à un observateur placé à une distance de visibilité maximale par rapport au pilote, conformément aux règles locales. Par exemple, si la limite de visibilité directe du drone est de 500 mètres par rapport au pilote, l'observateur se positionne alors à 500 mètres du pilote sur la trajectoire du drone ; lorsque le drone atteint cette distance, l'observateur se positionne 500 mètres plus loin, ce qui donne au pilote une visibilité directe de 1 km. L'observateur communique généralement avec le pilote pour l'informer du comportement du drone ; il peut aussi avoir une télécommande et prendre le contrôle du drone. Le pilote peut ensuite se placer 500 mètres après l'observateur, et ainsi de suite.
<b>F</b>	
<b>Champ de vision</b>	Mesure de l'amplitude visuelle à travers un viseur. L'unité généralement utilisée est le degré.
<b>Immersion</b>	Connexion sans fil entre le dispositif de prise de vue du drone et un écran situé soit sur la télécommande, soit sur un appareil fixé dessus (smartphone ou tablette), qui permet de visualiser ce que voit le drone. Le mode immersif est sujet à polémique car il implique qu'un pilote expérimenté pourrait laisser le drone aller au-delà de sa visibilité directe. Cela n'est toutefois pas évident et la plus grande prudence est de mise.
<b>Contrôleur de vol</b>	Microprocesseur ou « cerveau » du drone assurant le contrôle du vol.
<b>Domaine de vol</b>	Ampleur des manœuvres réalisables. Des limites sont fixées en ce qui concerne le roulis, le tangage et le lacet, afin de garantir la stabilité de l'aéronef.
<b>Fly Away</b>	Situation dans laquelle l'UAV échappe au contrôle de l'exploitant, souvent à cause d'interférences électroniques/magnétiques externes. Certains drones sont équipés de systèmes de protection contre ce type de situation. En cas de perte de contrôle, le système GPS des drones peut les faire revenir en toute sécurité sur leur point de départ.

<b>Châssis</b>	Voir « Cellule ».
<b>Saut de fréquence</b>	Changement de la fréquence d'émission d'un signal selon un schéma préétabli. Évite le non-aboutissement du signal sur une fréquence particulière.
<b>G</b>	
<b>Périmètre virtuel</b>	Limite géographique virtuelle définie par GPS qui, lorsqu'un appareil donné pénètre dans la zone ou en sort, déclenche chez lui une réaction.
<b>Cardan</b>	Support spécial d'un dispositif de prise de vues qui peut s'écarter et s'incliner sous l'action d'un servomoteur. Il permet au dispositif en question de rester dans la même position quels que soient les mouvements du drone, et donc de réaliser des images très nettes et fluides.
<b>Système de positionnement mondial (GPS)</b>	Ensemble de satellites en orbite à proximité de la Terre qui transmettent des signaux. Lorsque ces signaux sont reçus par un drone, ils déterminent sa position par rapport à la Terre.
<b>GLONASS</b>	Acronyme de <i>Globalnaya Navigazionnaya Sputnikovaya Sisyema</i> , ou système mondial de navigation par satellite. GLONASS est la version russe du GPS (Système de positionnement mondial).
<b>Poste de contrôle au sol (GCS)</b>	Voir « Poste de télépilotage (RPS) ».  <i>Note : « Poste de télépilotage » est l'expression privilégiée car elle peut s'appliquer de la même façon dans différents contextes (par exemple, sur un bateau ou un autre type d'aéronef).</i>
<b>Gyroscope</b>	Appareil mesurant la vitesse angulaire sur trois axes et permettant de maintenir l'orientation d'un quadricoptère.
<b>H</b>	
<b>Transfert</b>	Transmission du contrôle de pilotage d'un poste de télépilotage à un autre.
<b>Affichage tête haute</b>	Écran placé directement en face de la personne qui pilote un drone. Il peut afficher des données télémétriques comme l'altitude, la vitesse, l'angle de l'appareil, le cap et les coordonnées GPS. Voir aussi « Affichage à l'écran ».
<b>Hexacoptère</b>	Aéronef multirotor utilisant six rotors pour se déplacer dans l'air.

<b>Position d'origine</b>	Il s'agit soit du lieu d'où a décollé le drone et qui est stocké sur l'appareil, soit de l'endroit qui a été enregistré par l'utilisateur. Cette position est utilisée lorsque l'utilisateur actionne les commandes « Return to Home » (RTH) pour cause de batterie faible, « Failsafe RTH » lorsque le drone perd le signal de la télécommande pendant plus de 3 secondes, ou « Smart RTH » lorsque l'utilisateur appuie sur le bouton Home de la télécommande ou de l'application.
<b>Durée de vol stationnaire</b>	Durée pendant laquelle un drone peut rester immobile dans le ciel. Cette durée varie en fonction du poids de la charge utile : plus cette charge est lourde, et plus le vol stationnaire est de courte durée.
<b>I</b>	
<b>Indice de protection (IP)</b>	Indice utilisé pour définir le niveau de protection des dispositifs électriques contre l'intrusion d'éléments extérieurs (outils, saleté, etc.) et l'humidité. L'indice IP65 correspond par exemple à une protection contre les poussières et les jets d'eau à la lance.
<b>Unité de mesure inertielle</b>	L'accéléromètre et le gyroscope montés sur le contrôleur pour assurer l'orientation et la stabilisation consistent généralement en un ensemble d'au moins trois accéléromètres (qui mesurent le vecteur de gravité le long des axes x, y et z) et deux gyroscopes (qui mesurent la rotation autour des axes du roulis et du tangage). Cela n'est pas suffisant car les accéléromètres sont déstabilisés par le mouvement (ils sont brièvement « perturbés ») et les gyroscopes perdent leur axe au fil du temps. Les données de ces deux types de capteurs doivent être injectées dans le logiciel pour déterminer si le comportement et le déplacement de l'aéronef sont corrects.
<b>L</b>	
<b>Train d'atterrissage</b>	La plupart des drones possèdent un train d'atterrissage fixe, qui est également rétractable pour permettre une vision en vol sur 360 degrés. Les drones à voilure fixe n'ont pas de train d'atterrissage car ils se posent parfaitement sur le ventre.
<b>Batterie au lithium polymère (LIPO)</b>	Une variante est la batterie au lithium-ion (Li-Ion), qui est plus puissante et plus légère que les batteries au nickel-hydrure (NiMh) et au nickel-cadmium (NiCad).
<b>Visibilité</b>	Disposition réglementaire de première importance pour faire voler un UAV. Si l'aéronef ne se trouve pas dans l'axe de vision du pilote, ce dernier risque d'en perdre le contrôle et cela peut causer des accidents matériels ou de personnes.
<b>Défaillance de liaison (OACI)</b>	Perte de la liaison de contrôle et de commande avec l'aéronef télépiloté, de sorte que le télépilote ne parvient pas à gérer le vol.
<b>M</b>	
<b>Magnétomètre</b>	Boussole électronique utilisée par le contrôleur de vol pour connaître la direction.

<b>Multirotor</b>	Terme général désignant un drone possédant plus d'un moteur et d'une hélice pour assurer sa portance et sa propulsion. La plupart des drones courants possèdent au moins quatre rotors, mais ils peuvent aussi en avoir plus (jusqu'à 12, par exemple).
<b>N</b>	
<b>Nano</b>	Drone miniature pesant généralement moins de 8 grammes, et souvent classé dans la catégorie des jouets.
<b>Zone d'interdiction de survol</b>	Zone soumise à la réglementation de l'État, qui interdit ou désactive son survol par un aéronef (voir « Périmètre virtuel »).
<b>O</b>	
<b>Octocoptère</b>	Aéronef multirotor utilisant huit rotors pour se déplacer.
<b>Exploitant (OACI)</b>	Personne, organisme ou entreprise qui se livre ou propose de se livrer à l'exploitation d'un ou de plusieurs aéronefs.  <i>Note : Dans le contexte des aéronefs télépilotes, l'exploitation concerne également le système d'aéronef télépilote.</i>
<b>Affichage à l'écran</b>	Incrustation de données (souvent des données télémétriques) sur les vidéos envoyées au sol en temps réel par l'aéronef.
<b>P</b>	
<b>Charge utile</b>	Ce qui peut être transporté/soulevé/largué/livré par un drone.
<b>PIC (Pilot In Command)</b>	Désigne le commandant de bord, c'est-à-dire la personne légalement responsable car chargée du contrôle du drone à un moment donné.
<b>Pilote</b>	Personne chargée du contrôle direct d'un aéronef. Voir aussi « Télépilote ».
<b>Tangage</b>	Angle du drone en vol, qui fait qu'un bras est situé plus haut que les autres.
<b>Point d'intérêt</b>	Lieu qu'un UAV est censé atteindre. Peut aussi être un endroit sur lequel l'UAV doit effectuer des prises de vues.
<b>Carte de distribution</b>	Petit circuit imprimé utilisé pour organiser les connexions électriques et distribuer la puissance entre les batteries, le variateur de vitesse électronique et autres systèmes embarqués. Pas obligatoire sur tous les drones, mais courant sur les appareils de loisir pour que les connexions soient bien établies.
<b>Hélices</b>	Éléments permettant au drone de décoller du sol et de voler. Les hélices tournent en fonction des commandes manuelles du pilote, et l'intensité de leur rotation détermine l'ampleur de déplacement du drone.

<b>Régulateur à action proportionnelle, intégrale et dérivée (PID)</b>	PID désigne la formule mathématique utilisée par un contrôleur de vol pour obtenir un ratio puissance/réaction stable dans les moteurs d'un drone. L'ajustement de cette formule peut rendre un drone plus ou moins réactif, mais aussi moins stable.
<b>Q</b>	
<b>Quadricoptère</b>	Aéronef à voilure tournante. De conception plus simple qu'un hélicoptère télécommandé de la même taille, il est propulsé par quatre pales au lieu de deux.
<b>R</b>	
<b>Distance radio à portée optique (RLOS)</b>	Contact électronique direct, non entravé, entre un émetteur et un récepteur.
<b>Télécommandé</b>	Réception par un drone de ses instructions de vol par les ondes radio. Le pilote basé au sol peut utiliser un appareil portatif comme une manette de jeu ou, si le drone possède une connectivité wifi, un ordinateur ou une tablette.
<b>Prêt à voler (RTF)</b>	Drone ou quadricoptère dont le coffret comprend tout ce qu'il faut pour voler. Le kit inclut le drone, les batteries, le manuel d'utilisation, les systèmes de contrôle et tout autre équipement nécessaire pour faire voler l'appareil.
<b>Récepteur</b>	En règle générale, radio dont est équipé le drone et qui reçoit les commandes envoyées par l'émetteur de l'exploitant. Le récepteur peut aussi désigner le matériel vidéo/les lunettes utilisés par l'exploitant pour visualiser en immersion (voir ce terme) les vidéos envoyées en temps réel par le drone.
<b>Indicateur d'intensité du signal reçu (RSSI)</b>	Force du signal radio entre la télécommande et le drone.
<b>Return to Home (RTH)</b>	Fonction permettant de faire revenir le drone à sa position d'origine d'où il a décollé.
<b>Tours par minute (RPM)</b>	Nombre de fois où le moteur d'un drone effectue un tour complet pendant 60 secondes.
<b>Télépilote (OACI)</b>	Personne chargée par l'exploitant de fonctions indispensables à l'utilisation d'un aéronef télépiloté et qui en manœuvre les commandes, selon les besoins, durant le temps de vol.
<b>Poste de télépilotage (RPS)</b>	Composant du système d'aéronef télépiloté qui contient l'équipement utilisé pour conduire l'aéronef télépiloté.

<b>Système d'aéronef télépiloté*</b>	Système d'aéronef non habité incluant un certain nombre d'éléments tels qu'une unité de contrôle au sol, un système de lancement, le véhicule aérien sans pilote et tous les composants critiques permettant la sécurité des vols.
<b>Aéronef télépiloté (RPA) (OACI)</b>	Aéronef non habité piloté depuis un poste de télépilotage.
<b>Système d'aéronef télépiloté (RPAS). (OACI)</b>	Aéronef télépiloté, poste ou postes de télépilotage connexes, liaisons de commande et de contrôle nécessaires et tout autre composant spécifié dans la conception de type approuvée.
<b>Roulis</b>	Terme de navigation aérienne désignant la rotation autour de l'axe longitudinal, provoquant l'inclinaison du drone d'un côté à l'autre.
<b>Aéronef à voilure tournante</b>	Véhicule aéroporté dont la portance et la propulsion sont assurées par les pales d'un rotor, et non par des ailes comme sur un avion. Lorsque la voilure tournante est composée de deux pales ou plus, l'aéronef est dit multirotor.
<b>Observateur RPA (OACI)</b>	Personne formée et compétente désignée par l'exploitant, qui, par observation visuelle de l'aéronef télépiloté, aide le télépilote à assurer la sécurité de l'exécution du vol.
<b>Commandant de RPAS *</b>	Chargé d'assurer la conduite et la sécurité d'un vol particulier, ainsi que de superviser le pilote du système d'aéronef télépiloté (RPAS). Ses tâches sont équivalentes à celles du commandant d'un avion.
<b>RTK (cinématique en temps réel)</b>	Mode de navigation par satellite utilisé pour accroître la précision des données de position fournies par des systèmes de positionnement s'appuyant sur des systèmes de précision comme le GPS.
<b>Gouvernail</b>	Voir « Lacet ». Détermine la direction du drone.
<b>S</b>	
<b>Voir et éviter</b>	Voir « Détection et évitement ».
<b>Servomoteur</b>	Dispositif mécanique utilisé parfois sur les drones pour actionner des éléments ou des surfaces. La plupart des drones n'ont pas besoin d'un servomoteur car leurs déplacements sont gérés en modifiant la vitesse de chaque rotor. Un servomoteur est plus justifié sur les aéronefs à voilure fixe ou les cardans.
<b>Petit aéronef non habité (SUA)</b>	Aéronef sans pilote autre qu'un ballon ou un cerf-volant, pesant moins qu'un certain poids fixé par chaque pays, en excluant le carburant mais en incluant tout article ou équipement installé ou fixé sur l'aéronef avant le début du vol.



<b>Petit aéronef de surveillance non habité (SUSA)</b>	Petit aéronef sans pilote équipé pour effectuer des missions de surveillance ou d'acquisition de données.
<b>Essaim</b>	Terme technique désignant un ensemble d'UAV dirigés par intelligence artificielle. Les drones en essaim communiquent entre eux pendant le vol et peuvent réagir seuls en cas d'évolution du contexte. Un essaim de drones est semblable à une dense nuée d'étourneaux réagissant à la menace soudaine d'un faucon. L'ensemble de la nuée se meut comme s'il s'agissait d'un seul individu. Ne pas confondre un essaim de drones avec un groupe d'UAV volant ensemble en formation et agissant chacun de leur côté de façon autonome.
<b>T</b>	
<b>Données télémétriques</b>	Ensemble de données mesurant tous les paramètres du vol d'un drone : vitesse, altitude, axes de roulis, tangage et lacet, autonomie de la batterie, position, etc.
<b>Système thermique</b>	Une caméra thermique collecte des images et des données thermiques. Elle peut être utilisée pour inspecter des bâtiments industriels, vérifier des cultures agricoles ou, plus classiquement, détecter des traces de vie dans des situations de crise.
<b>Commande des gaz</b>	Manette de contrôle de la vitesse des hélices/moteurs, mesurée par le nombre de tours par minute. Lorsque ces données sont interprétées par le contrôleur de vol, elles peuvent permettre de modifier l'altitude ou la trajectoire du drone, par exemple.
<b>Émetteur</b>	Autre nom pour « Télécommande ». Permet de contrôler le drone en vol depuis le sol.
<b>Compensation</b>	Ajustement permettant de modifier la base du levier d'une télécommande. Si le drone a tendance à « dériver » dans une certaine direction lorsque le levier n'est pas maintenu par l'utilisateur, ce dernier peut opérer une « compensation » du levier afin que le drone maintienne sa position même lorsque l'utilisateur ne touche pas la télécommande.
<b>Mode Tripod</b>	Mode stable et très lent, idéal pour capturer des images près du sol et réaliser des gros plans. Mode permettant une très grande précision, qui est souvent utilisé par les réalisateurs de films et les photographes dans leur travail.
<b>U</b>	
<b>Pilote d'UAV</b>	Voir « Pilote ».

<b>Aéronef sans pilote</b>	<p>Aéronef conçu pour naviguer sans pilote à son bord, au sein d'un système d'aéronef non habité. Ses caractéristiques :</p> <ul style="list-style-type: none"> <li>- Capacité à voler un certain temps grâce à ses propriétés aérodynamiques ;</li> <li>- Pilotable à distance ou capacité à voler de façon autonome ;</li> <li>- Réutilisable, et</li> <li>- Non classé dans la catégorie des armes téléguidées ou autres dispositifs à usage unique conçus pour transporter des munitions.</li> </ul> <p><i>Note : Un véhicule aérien sans pilote est considéré comme une sous-catégorie des aéronefs sans pilote.</i></p>
<b>Système d'aéronef non habité</b>	<p>Ce système comprend plusieurs éléments indépendants : l'aéronef sans pilote et tout ce qui lui permet de voler (poste de télépilotage, liaison de communication, élément de décollage et d'atterrissage). Le système d'aéronef non habité peut inclure plusieurs aéronefs, postes de télépilotage et éléments de décollage et d'atterrissage.</p>
<b>V</b>	
<b>VLoS</b>	<p>Acronyme désignant le vol en visibilité directe, c'est-à-dire le contraire de BVLoS (Au-delà de la visibilité directe). C'est le mode qui doit être utilisé par un exploitant pour faire voler un drone, c'est-à-dire en maintenant un contact visuel direct avec lui.</p>
<b>Décollage et atterrissage verticaux (ADAV)</b>	<p>Cette caractéristique des quadricoptères et autres UAV équipés de plusieurs rotors est très utile, car elle leur permet de décoller et d'atterrir avec très peu d'espace disponible. Ce n'est pas le cas des aéronefs à voilure fixe, qui ont besoin d'une piste pour décoller et atterrir.</p>
<b>Vol en visibilité directe (VLOS) (OACI)</b>	<p>Vol durant lequel le télépilote ou l'observateur RPA maintient un contact visuel direct avec l'aéronef télépiloté.</p>
<b>W</b>	
<b>Point de passage</b>	<p>Ensemble de trois coordonnées ou plus servant à guider un drone le long d'un itinéraire de vol fixé à l'avance pour des missions en autonomie.</p>
<b>Pleins gaz</b>	<p>Correspond au régime maximal d'un drone, que l'on enclenche en poussant complètement vers l'avant le levier de la télécommande.</p>
<b>Y</b>	
<b>Lacet</b>	<p>Terme de navigation aérienne désignant la rotation d'un drone autour de son axe vertical. Détermine la direction du quadricoptère.</p>

-----



INTERPOL

Relier les polices pour un monde plus sûr



[WWW.INTERPOL.INT](http://WWW.INTERPOL.INT)



[INTERPOL\\_HQ](https://www.instagram.com/INTERPOL_HQ)



[@INTERPOL\\_HQ](https://twitter.com/INTERPOL_HQ)



[INTERPOLHQ](https://www.facebook.com/INTERPOLHQ)



[INTERPOLHQ](https://www.youtube.com/INTERPOLHQ)