< PLAN DE TESTS & ANALYSES DE SÉCURITÉ SUR LE DRONES >

CAMPUS CYBER 2026

< SOMMAIRE >

< 1. DÉFINITIONS >

Un drone se définit généralement comme un « engin mobile terrestre, aérien, naval ou spatial, sans équipage embarqué, programmé ou télécommandé, et qui peut être réutilisé. » [1]

La définition de la CNIL apporte des précisions supplémentaires ; un drone est « un appareil sans pilote à bord. Il est généralement piloté à distance par un opérateur humain, mais peut avoir un degré plus ou moins important d'autonomie (par exemple pour éviter des collisions ou gérer les conditions aérologiques). Un drone est avant tout une plateforme de capteurs mobiles. C'est un engin d'observation, d'acquisition et de transmission de données géolocalisées. » [2]

Il peut être de plusieurs types : aérien, terrestre, marin/sous-marin. Le plus commun et principalement associé au nom "drone" est le quadricoptère, dont la présence dans les usages personnels et professionnels n'a cessé de croitre ces dernières années.

L'objectif du Groupe de travail « Etat de l'art des attaques et défenses sur les drones », rattaché à la Communauté d'Intérêt « Sécurisation des drones et robots » du Campus Cyber, est d'identifier l'ensemble des mécanismes de sécurités pouvant - et devant ! - être positionné sur l'environnement « drone », de l'appareil lui-même à tout les éléments associés à celui-ci. Cet inventaire précède la création d'une méthode de contrôle de l'état de sécurité de l'appareil.

En dressant l'état de l'art des attaques sur les drones civils (terrestres/aériens/marins...), le GT a designé un plan de tests et effectué des analyses de sécurités techniques (statiques et dynamiques) sur deux drones à sa disposition, afin de proposer des contre-mesures. Il s'agissait de drones « grand public » : le DJI 3 et le Parrot Anafi (ce dernier étant équipé d'une connectique 5G).

1. Wiktionnaire. (2026). Drone. Disponible sur : https://fr.wiktionary.org/wiki/drone
2. CNIL. (2026). Drone. Disponible sur : https://www.cnil.fr/fr/definition/drone

< 2. DÉMARCHE GÉNÉRALE >

Pour dresser l'état de l'art et des mesures de contrôle de sécurité dans ce domaine varié, il a fallu élaborer une démarche générale capable de s'adapter à la diversité des environnements et aux risques spécifiques à chacun. En s'inspirant de la méthode utilisée pour établir une Politique de Sécurité des Systèmes d'Information (PSSI), l'analyse des risques apparaît comme une étape indispensable pour assurer une couverture technique exhaustive et rigoureuse par la suite.

Pour répondre à ces enjeux, nous avons décidé de réaliser une analyse macroscopique sur les différents types d'environnements existants, puis de construire un plan de test basé sur cette analyse afin de couvrir techniquement leurs contrôles. Le cycle de cette démarche est le suivant :

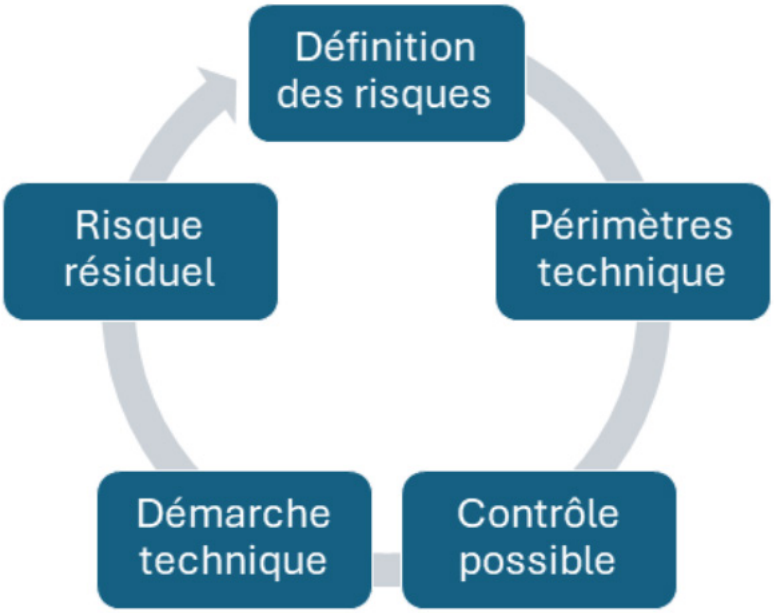

Figure 1 : Schéma de l'analyse macroscopique

Chacune de ces étapes se définie comme suit :

- **Définition des risques :** définir l'ensemble des sources de risques (SR) et objectifs visé (OV), permettant d'identifier un ensemble d'évènements redoutés devant être couvert par des contrôles technique afin d'en assurer l'état de sécurité et la couverture du risque ;
- **Périmètre technique** : pour chacun de ces évènements redoutés, identifier des périmètres techniques concernés, sans distinction préalable de la typologie du drone ;

- **Contrôle possible** : ensemble des contrôles pouvant être mis en œuvre sur les périmètres techniques précédents pour répondre aux risques définis ;
- **Démarche technique :** détail et procédure de réalisation des tests techniques nécessaire au contrôle, permettant de qualifier le niveau de risque ;
- **Risque résiduel :** risque restant dans le cas où le contrôle ne permet pas d'assurer une couverture totale du risque initial.

L'objectif du GT est de construire la démarche de test, exprimée dans un cahier de test, devant servir de socle technique pour la réalisation d'un audit de l'état de sécurité d'un drone cible.

Cette démarche est agnostique : elle ne tient pas compte de la typologie ou de l'usage du drone, ni des attentes spécifiques pouvant exister. Elle se veut la plus générique possible, pour en assurer l'application dans la majorité des situations.

< 3. APPROCHE PAR LES RISQUES >

La démarche générale de couverture sécurité a été conçue grâce à une approche initiale par les risques, en s'inspirant de la méthode EBIOS Risk Manager 2018. Un cadrage du système « Drone » a été réalisé. Cela a permis d'identifier les valeurs métiers et les biens supports liés à l'usage de drones, les évènements redoutés principaux et de définir le niveau d'impact pour l'ensemble des risques.

3.1 DÉFINITION DES TERMES

- **Valeurs métiers** : composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle ;
- **Biens supports** : dans le cadre de l'étude, composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé.

En début de ce livrable, le drone a été décrit en reprenant deux définitions : celles de Wiktionary et de la CNIL comme référence. Dans le cadre de ce groupe de travail, le drone est également compris comme remplissant des missions pour des entreprises et des collectivités, dans tout domaine d'application (hors domaine militaire et régalien), et réalisant des captation, transmission et/ou action (exemple : épandage).

3.2 CHOIX DE LA MÉTHODE D'ANALYSE DE RISQUE

La méthode EBIOS Risk Manager 2018, méthode de référence en France proposée par l'ANSSI, a été selectionnée. Elle est en effet maitrisée par les membres du GT et offre une importante flexibilité, sur un grand nombre de contexte et cible.

L'objectif de cette étape étant de cadrer le reste des actions, l'analyse de risque s'est limitée à un cadrage du système « Drone ». Les valeurs métiers, les biens supports et des évènements redoutés ont été définis en visant le plus large spectre possible pour permettre à chacun d'appliquer la démarche de test à sa situation, sans contraintes de typologies, contexte, milieu ou usage.

3.3 CADRAGE DU SYSTÈME

En termes de valeurs métiers, il a été identifié :

- Déplacement [Processus], sa capacité à se déplacer dans l'espace (3D) selon son type terrestre, aérien ou marin.
- Affichage imagerie drone [Processus], sa capacité à afficher les données récupérées par le drone.
- Transmission de données [Processus], sa capacité à transmettre bilatéralement des données sur les canaux télécommande - cloud et télécommande - drone.
- Acquisition de l'imagerie [Processus], sa capacité à récupérer des données via ses capteurs embarqués
- Transport [Processus], sa capacité à transporter de charges ou équipements tiers ou des personnes.
- Fonctionnalités de sécurité [Processus], c'est-à-dire que le drone doit respecter les zones de survol interdit, avoir des fonctionnalités d'évitement en l'air et d'évitement d'obstacles, etc.
- Utilisation des modules complémentaires [Processus], par exemple un système d'épandage, un drone démineur etc.
- Données issues des capteurs [Information] que ce soient l'imagerie (caméra ...), les données GPS et de positionnement ou les données gyroscopiques
- Cartographie interne [Information], utilisée à la fois dans le plan de vol et pour la gestion des zones de survol interdit

A travers toutes ces valeurs métiers, c'est l'utilité du drone qui est identifiée.

Pour mettre en évidence ce raisonnement, les biens supports relatifs à l'acquisition de l'imagerie ont été particulièrement étudiés tels que :

- Batterie, permet d'alimenter tous les autres biens supports ;
- Caméra, permet d'acquérir des données visuelles ;
- Contrôleur de vol, permet de piloter l'acquisition de l'imagerie et de contrôler les capteurs internes (gyroscope, retours moteurs, accéléromètre, thermomètre, …) ;
- GPS hardware, permet d'acquérir des données de localisation GNSS ;
- GPS software drone, permet d'acquérir des données de localisation GNSS ;
- Mémoire drone hardware, permets de stocker les données récoltées.

Vient ensuite les évènements redoutés, ou comment un acteur malveillant pourrait nuire.

Deux relatifs à l'acquisition de l'imagerie ont été relevés :

- Une atteinte à l'intégrité des biens supports relatifs à l'acquisition de l'imagerie soit le dysfonctionnement/sabotage de capteurs :
  - Altération ou brouillage des capteurs (GNSS spoofing) ;
  - Erreurs de navigation, mauvaises décisions en vol, collisions ou pertes de cible ;
  - Gyroscope qui s'inverse

- Une atteinte à la disponibilité des biens supports relatifs à l'acquisition de l'imagerie soit l'aveuglement de capteurs :
    - Arrêt de différents capteurs (Gyroscope, caméra (MRA), GPS ou retours moteurs)

3.4 ÉCHELLE ET RÉSULTATS

Pour chaque évènement redouté, un impact a été assigné selon cette échelle d'impacts :

NIVEAU	INTITULÉ	DESCRIPTION	COULEUR
1	Mineure	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés (consommation des marges).	
2	Significative	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. L'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).	
3	Grave	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.	
4	Critique	Incapacité pour l'organisation d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. L'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.	

Ces éléments se veulent généralistes et devront être adaptés à chaque audit en fonction du contexte prévu d'utilisation d'un drone - en particulier, le niveau de gravité associé à chaque évènement redouté.

A la suite de cette analyse, plusieurs axes sur lesquels travailler ont été identifiés :

- Interfaces sans fil ;
- Protocoles de communication ;
- Interfaces logicielles ;
- Résistance physique et sécurité ;
- Résilience aux cyberattaques.

Les parties suivantes détaillent l'élaboration du plan de test à partir des risques identifiés ainsi que la démarche technique déroulée sur deux modèles de drones.

< 4. CONSTRUCTION DE LA MÉTHODE D'AUDIT >

A la suite de la réalisation de l'analyse de risque, la construction d'un cahier de test a été initiée. Celui-ci reprend les résultats de l'analyse et défini un ensemble de 5 catégories principales à couvrir par plusieurs tests techniques.

Les catégories ont été regroupés selon le modèle suivant :

- **Interfaces sans fil :** comprenant toute canal de communication entrant / sortant du drone via des technologies radio, propriétaire ou publique. On y retrouve les réseaux Wi-Fi et Bluetooth, mais également les interfaces radio plus classique.

- **Protocoles de communication** : contrôle de la sécurité des protocoles, public ou propriétaires exploitées pour le contrôle mais également pour le partage d'information, tel que la transmission vidéo.

- **Interfaces logicielles :** toutes solutions logicielles permettant un contrôle total ou partiel du drone, dont la compromission pourrait impacter le fonctionnement, la confidentialité.

- **Résistance physique et sécurité** : protection technique du drone, et des composant tier, y compris la transmission de donnée dès lors qu'elle n'est pas sans fil. La résistance aux analyses forensique est également associés à cette catégorie.

- **Résilience aux cyberattaques** : contrôle des réactions du drone lors de mise en œuvre d'attaque, principalement des brouillage et tentative de prise de contrôle.

Pour chacune de ces catégories un ensemble de tests macroscopiques a été identifié, et la profondeur des tests est au modulo du besoin de sécurité et au risque de l'utilisateur. La démarche technique reprend ces catégories et tests afin de détailler l'ensemble des contrôles techniques pouvant être mis en œuvre pour couvrir les risques.

C'est l'exploitation de cette démarche technique qui produit l'analyse générale de l'état de sécurité du drone et dont les résultats permettent d'identifier les actions de mises en sécurités nécessaires, l'acceptation du risque ou bien le rejet d'un drone insuffisamment sécurisé.

La démarche a été conçue de manière à présenter les outils et plan d'action pour la mise en œuvre du contrôle. L'objectif était également de lister les résultats attendus dans le cas d'un niveau de sécurité estimé suffisant, ainsi que les constats mettant en avant l'absence de contrôle ou de protection.

< 5. DÉMARCHE DE TESTS ET HYPOTHÈSE DE SÉCURITÉ >

Les catégories précédemment identifiées ont par la suite été associés aux différents types d'attaque possible, dans le contexte d'une exploitation sur drone, afin d'en dresser un panorama des hypothèses de sécurité à couvrir (en fonction de l'usage et du scénario d'exploitation).

L'idée est de proposer une démarche dont la complexité, liée directement à la profondeur de couverture, est associés à une typologie d'attaque réaliste dans le contexte de l'utilisateur.

A titre d'exemple, pour chacune des catégories les principales attaques retenues sont les suivantes :

Interface sans fil :

- Exploitation de vulnérabilité/faiblesse permettant à un acteur malveillant d'établir une liaison avec le drone, ou bien intercepter des communications ;
- Exploitation des configurations usines potentiellement faibles ;
- Risque : fuite des données du drone et/ou de la télécommande. Prise de contrôle à distance du drone par un acteur non autorisé via connexion abusive à l'interface radio. Interception ou manipulation des données échangées, pouvant exposer des informations sensibles (télémétrie, localisation, flux vidéo). Déni de service par saturation ou perturbation volontaire des interfaces de communication ;
- Réalisation : utilisation d'outils spécialisés d'audit d'interfaces sans fil, tel que SDR, interface Wi-Fi, sniffer bluetooth, IMSI catcher ;
- Complexité : simple pour les protocoles les plus commun (wifi, bluetooth) et un contrôle rapide. Monte rapidement en complexité si nécessaire de basculer sur des technologies GSM, propriétaires, etc.

Protocole de communication :

- Exploitation d'une absence de chiffrement, ou d'un chiffrement faible, pour accéder au contenu des communications ;
- Contrôle de la protection anti-rejeu des commandes de pilotages ;
- Risque : prise de contrôle du drone par un acteur malveillant. Injection ou modification de commandes, en l'absence de mécanismes d'intégrité ou d'authentification forte. Rejeu de commandes (replay attack) si la protection anti-rejeu est insuffisante, permettant de répéter des actions antérieures. Compromission du canal de pilotage, entraînant une perte de maîtrise du drone. Lecture non-autorisée de données sensibles transmises en clair (données GPS, flux vidéo, paramètres techniques) ;
- Réalisation : analyse des protocoles exploités pour identifier l'absence de mécanisme de sécurité conforme à l'état de l'art (chiffrement, faible entropie, absence d'intégrité, absence de challenge-réponse, etc.)
- Complexité : moyenne à avancée - dépend de la sophistication du protocole (propriétaire, standard, chiffré, documenté ou non)

Interfaces logicielles :

- Faiblesse dans les applications de pilotage, configuration, gestion du drone, pouvant mener à des modifications d'aspect de sécurité, du firmware de l'appareil, etc.
- Risque : perte de contrôle du drone. Bypass ou affaiblissement de mécanisme de sécurité, fuite d'information sensible, perte de contrôle du drone.
- Réalisation : audit de sécurité des différentes applications logicielles annexes au drone.
- Complexité : moyenne - variable en fonction des technologies employées (smartphone, application web, etc.)

Résistance physique et sécurité :

- Accès physique au drone permettant la modification des composants, ports de maintenance, carte mémoire, firmware, capteurs.
- Risque : sabotage. Extraction de données internes, notamment logs, clés de chiffrement, informations de configuration. Modification du firmware par accès physique direct, rendant possible une prise de contrôle persistante.
- Réalisation : inspection physique du drone pour identifier les interfaces accessibles physiquement et contrôler leur sécurité. Identification des mécanismes de protection physique mis en place.
- Complexité : faible à avancée, dépend de la protection physique appliquée par le constructeur et des interfaces accessibles.

Résilience aux cyberattaques :

- Contrôle du comportement du drone en cas de brouillage actif des communications de commande, GPS, réseau générale (Wifi, 4G, ...)
- Risque : perte de contrôle du drone. Comportement non maitrisé / non attendu du drône en cas d'attaque logique et absence de maitrise ou de préparation à l'évènement
- Réalisation : la conduite d'action de brouillage est fortement encadrée et nécessite des infrastructures spécifiques pour être réalisé. Il est nécessaire d'isoler l'équipement cible et la source du brouillage dans une cage de faraday pour éviter le débordement du brouillage.
- Complexité : avancée - nécessite des environnements très contrôler pour effectuer les tests.

Un plan de test doit être établi à l'aide de ces différents éléments, en fonction des risques préalablement identifiés et des besoins / contraintes opérationnels propre à l'acteur souhaitant se munir de drone pour ses activités. L'analyse de risque préalable étant un des éléments principaux pour dicter cette sélection et la profondeur des contrôles.

Selon les usages envisagés, les préoccupations en matière de sécurité sont amenées à varier, tout comme les exigences de confidentialité. La définition précise du périmètre de contrôle permet ainsi de concentrer l'évaluation sur les aspects réellement critiques pour l'acteur.

< 6. POUR ALLER PLUS LOIN >

Le GT n'a pas été en mesure de réaliser une version complète du cahier de tests ainsi que sa mise en œuvre sur les équipements acquis par le Campus Cyber dans cet objectif. La continuité de celui-ci dans l'activité des groupes d'expert du Campus Cyber pourra être envisagée. Quelques pistes ont été évoquées :

- Une mise en application du cahier de test sur des appareils de plus grandes envergures associées au domaine de la mobilité ;
- Une amélioration du cahier de test, englobant un plus grand nombre de domaines techniques.

Dans l'attente d'une éventuelle reprise des travaux par le Campus, ce livrable peut être exploité et enrichi par une vaste typologie d'acteurs. Toute proposition d'amélioration peut être soumise au groupe de travail et sera étudiée par les équipes impliquées dans les futures avancées.

Le Campus Cyber tient à remercier l'ensemble des contributeurs du GT, dont Baptiste DESEAU LE REST (I-Tracing), Paul T., Paul Sarou (EDF), Hamza GUEFIF (UTAC), Guillaume JACQUEMIN (UTAC) et José LOPES-ESTEVES (ANSSI). Le Campus remercie également Fabien CAURA et Aline BECQ pour le soutien et l'accompagnement offert par le LabCyber, programme opéré par le Programme de Transfert au Campus Cyber.

< 7. RÉFÉRENCES>

- ANSSI. (2028). La méthode EBIOS Risk Managaer - Le guide. Disponible sur : https://messervices.cyber.gouv.fr/guides/la-methode-ebios-risk-manager-le-guide
- OWASP. (2022). Hacking the Drones. Disponible sur : https://owasp.org/www-chapter-london/assets/slides/OWASP201604_Drones.pdf
- Pentest Magazine & courses. (2024). Aerial Assault: Combining Drone and Pentesting (W54). Disponible sur : https://pentestmag.com/product/aerial-assault-combining-drones-and-pentesting-w54/
- Wiktionary. (2026). Drone. Disponbile sur : https://fr.wiktionary.org/wiki/drone

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CAMPUS CYBER 2026 © - PLAN DE TESTS & ANALYSES DE SÉCURITÉ SUR LES DRONES

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT
DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR

CC BY SA