Évaluation et comparaison des technologies d'atténuation des contre-drones (C-UAS)

Quelle technologie de lutte contre les drones est la plus adaptée au cas d'utilisation et au scénario ? Cette note blanche évalue les forces et les faiblesses des technologies existantes et récentes, afin de contribuer à éclairer les discussions et les évaluations concernant la technologie qui répondra le mieux à des besoins spécifiques.

Brouilleurs de radiofréquence (RF)

Technologie d'atténuation	Défi majeur
Brouilleurs de radiofréquence (RF)	Interférences de communication/ GNSS

Les brouilleurs RF canalisent de grandes décharges d'énergie RF qui masquent le signal du contrôleur et empêchent le drone de recevoir des instructions. Certains brouilleurs concentrent leur rayonnement en direction du drone.

Cette technologie est relativement bon marché, simple à utiliser et peut produire un effet souhaité : la neutralisation temporaire de tous les drones à proximité immédiate. Ce sont des avantages intéressants, mais ils s'accompagnent de quelques inconvénients importants.

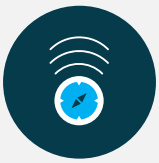
Le bruit RF peut interférer avec les systèmes de communication et/ou GNSS à proximité, rendant cette technologie d'atténuation problématique dans de nombreux environnements sensibles, notamment la possibilité d'arrêter des drones amis et autorisés.

Comme l'effet de brouillage dépend de la force du bruit RF créé par le brouilleur, son effet repose sur la force relative des signaux que le drone reçoit du dispositif de télécommande et du brouilleur, et cela dépend à la fois de la puissance de transmission et de la distance au drone. Le brouilleur ne fonctionne que si son signal est prédominant. Cette condition a plusieurs répercussions :

- Le brouilleur ne fonctionnera que lorsque le drone sera suffisamment éloigné de son dispositif de télécommande mais suffisamment proche du brouilleur
- Si le drone est sur la route du retour, son pilote peut reprendre le contrôle une fois que le drone se rapproche suffisamment du dispositif de télécommande
- Si le brouilleur cesse de transmettre, le pilote peut immédiatement reprendre le contrôle ; cette méthode dépend d'une transmission continue

Les brouilleurs ne prennent pas le contrôle d'un drone ; ils se contentent de le déconnecter de son dispositif de télécommande. Une fois déconnecté, il essaie généralement de revenir à sa position de décollage (« d'origine »), mais peut également voler sur place ou tenter d'atterrir. Certains drones peuvent être programmés pour exécuter d'autres actions d'urgence par défaut. Chacune de ces options peut constituer une menace (par exemple, un drone rentrant chez lui peut survoler un espace aérien sensible comme le couloir de décollage d'un aéroport) ; lorsque le drone vole sans contrôle, même son pilote ne peut prévenir les dommages. À moins que le drone ne soit à portée de vue, l'opérateur du brouilleur peut même ne pas savoir si le drone a été déconnecté. Les brouilleurs n'éliminent pas toujours définitivement la menace spécifique, mais la bloquent seulement temporairement, car dans de nombreux cas, le drone reviendra vers son pilote.

Différents types de brouilleurs présentent des points forts et des faiblesses spécifiques :



Brouilleurs directionnels

Ces brouilleurs atténuent les drones arrivant d'une direction spécifique. Cette technologie offre une portée plus longue que les autres types de brouillage et provoque moins de perturbations et d'interférences de signal dans l'environnement immédiat. Elle requiert une transmission continue pour demeurer en vigueur. Elle ne peut pas, à elle seule, se débarrasser de hordes qui, de par leur nature, s'approchent généralement de plusieurs directions.

Un faisceau étroit peut également perdre son efficacité si le drone commence à retourner vers son lieu d'origine, et le pilote peut reprendre le contrôle et voler dans une direction différente ou échapper à l'angle effectif du brouilleur directionnel.

Brouilleurs omnidirectionnels

Les brouilleurs omnidirectionnels peuvent réduire les drones venant de toutes les directions et ainsi mieux gérer les hordes. Mais ils offrent une portée plus courte que les brouilleurs directionnels, ce qui signifie que la zone protégée est plus petite.

La transmission omnidirectionnelle accroît également l'effet collatéral sur les drones autorisés et non menaçants, ainsi que sur les autres systèmes de communication à proximité.

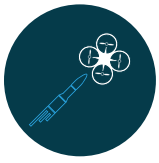
Brouilleurs portatifs

Ces brouilleurs sont mobiles et simples à utiliser. Il suffit à l'opérateur de sortir le dispositif et de le pointer. Inconvénients : Cette méthode étant manuelle, un membre de l'équipe de sécurité doit toujours porter le brouilleur portatif sur lui/elle et demeurer vigilant.

Si l'opérateur ne peut pas activer immédiatement le brouilleur portatif ou n'y prête pas attention, la possibilité d'atténuer le drone malveillant pourrait rapidement se perdre. De plus, les brouilleurs portatifs fonctionnent à un faible niveau de puissance afin de ne pas compromettre la santé de l'opérateur, mais également de limiter la portée du dispositif.

Ce type de brouilleur est efficace dans les scénarios où un certain point sensible doit être protégé et où les drones menaçants sont à proximité et à portée de vue. C'est pratiquement inutile dans les cas où un périmètre ou une frontière doit être défendue car le drone peut simplement voler assez haut pour être hors de portée du brouilleur portatif.

Solutions cinétiques

Technologie d'atténuation	Défi majeur
 Solutions cinétiques	 Requiert une ligne de mire

Les solutions cinétiques empêchent le drone de fonctionner par une sorte d'intervention physique, par exemple un projectile. Elles varient en taille et en portabilité, en facilité d'utilisation, en coût et en capacités par rapport à des types de drones spécifiques.

De manière moins favorable, certaines technologies cinétiques, mais pas toutes, peuvent requérir une visibilité directe, ce qui n'est pas toujours disponible dans les environnements urbains ou sensibles en raison des gratte-ciel, des véhicules, de la signalisation, etc.

Les solutions cinétiques visent, dans la plupart des cas, à faire tomber le drone du ciel, ce qui peut causer de graves dommages collatéraux ou des blessures humaines. Les projectiles eux-mêmes peuvent également toucher d'autres objets et présenter un risque, notamment dans des environnements sensibles tels que les aéroports ou les infrastructures essentielles.

Comme pour les brouilleurs, différents types de solutions cinétiques présentent des avantages et des inconvénients associés :

Drone tueur de drones (filet de remorquage, collision, lancer de filet ou projectile)

Les drones tueurs de drones peuvent capturer des cibles non autorisées avec des filets et les remorquer jusqu'à un atterrissage contrôlé. Alternativement, cette catégorie peut également comprendre des drones qui tentent de percuter des drones malveillants et de les désactiver. Enfin, certains de ces drones défensifs peuvent tirer des filets ou d'autres projectiles vers des drones non autorisés. Les frappes précises peuvent s'avérer difficiles pour ces méthodes lorsqu'il s'agit de contrer un drone qui vole de manière imprévisible.

Le drone tueur doit « engager un combat aérien » ou chasser le drone malveillant, et il est extrêmement difficile de le faire par le biais d'un système autonome ou via des drones contrôlés par un pilote depuis le sol. Cette méthode peut également entraîner des dommages collatéraux dus à la chute libre d'un drone et d'un projectile.

Tireur intelligent

Les tireurs intelligents disposent d'un système monté sur un fusil qui permet des tirs précis contre les drones à proximité. Une lunette spéciale exécute un calcul avant le tir. La probabilité d'une frappe, par rapport aux autres méthodes cinétiques, est donc accrue. Cette technologie est plus économique et peut jouer un rôle dans un système anti-drone multicouche, en particulier dans les environnements ruraux ou à découvert. Cette technologie est précise jusqu'à quelques centaines de mètres (généralement moins de 250 mètres) et est susceptible de rencontrer des difficultés pour toucher de plus petits drones. L'équipe de sécurité doit agir immédiatement - les drones volent vite et il n'y a que quelques secondes pour riposter.

Lasers

Technologie d'atténuation	Défi majeur
 Lasers	 Précision affectée par les conditions météorologiques

Ces dispositifs haute énergie justifient leur propre sous-catégorie. En émettant un intense faisceau de lumière, les systèmes laser peuvent détruire la structure du drone ou ses composants électroniques. Les lasers détruisent les drones et peuvent affronter de nombreux types de drones. Par contre, ils requièrent une ligne de mire, réduisent le drone en cendres (détruisant l'intelligence) et peuvent également entraîner la chute de fragments de drone. Des dommages collatéraux sont possibles et des obstacles tels que des immeubles ou d'autres objets volants peuvent poser des problèmes.

C'est pour ces raisons que les lasers peuvent, dans certains cas, convenir moins aux environnements sensibles. Il est également plus difficile d'atteindre de plus petits drones à l'aide de lasers.

Impulsion électromagnétique (EMP)/Micro-ondes haute puissance (HPM)

Technologie d'atténuation	Défi majeur
 Impulsion électromagnétique (EMP)/ Haute puissance	 Micro-ondes (hpm) et dégâts collatéraux importants

Il s'agit d'une technologie fondée sur les rayonnements. Elle utilise une explosion d'énergie électromagnétique de haute puissance en rafales courtes, endommageant potentiellement tout le système électrique de la zone. L'EMP fonctionne sans distinction et peut causer de lourds dommages collatéraux. Par exemple, elle peut endommager de manière permanente les appareils électroniques ou les ordinateurs à proximité, en endommageant leurs circuits. L'EMP est souvent considérée comme une option de dernier recours.

Usurpation/spoofing GNSS

Technologie d'atténuation	Défi majeur
 GNSS électromagnétique	 Peut provoquer des accidents

L'usurpation du système mondial de navigation par satellite (GNSS) diffuse un faux signal GNSS tel que le GPS dans une zone spécifique. Un récepteur GNSS qui reçoit le signal usurpé peut erronément déterminer sa localisation. En contrôlant la localisation perçue d'un drone, il peut être possible de le faire voler dans une direction souhaitée et ainsi de le diriger. Alternativement, cela peut empêcher le drone de voler selon un plan de vol préprogrammé ou de rentrer à sa base.

En termes de perturbation de l'environnement et d'incidence sur la continuité, cette technologie peut s'avérer encore plus problématique que le brouillage. Chaque système de navigation dans la zone peut recevoir le signal GPS usurpé et déterminer une position globale erronée.

L'usurpation GPS pourrait affecter, par exemple, les systèmes de navigation des voitures de civils ou les applications de navigation des conducteurs, provoquant ainsi de la confusion, des accidents et pire encore. Elle pourrait également perturber le fonctionnement des drones amis. Cette technologie ne doit évidemment pas s'utiliser à proximité de navires, avions ou hélicoptères amis autorisés.

Cyber-prise de contrôle RF

Technologie d'atténuation	Défi majeur
 Cyber-prise de contrôle	 Surmonter les protocoles avancés des drones

La cyberprise de contrôle RF est une technologie sans brouillage et non cinétique qui transmet un signal précis et court qui prend le contrôle du drone malveillant. Cette technologie se focalise sur les communications RF entre le dispositif de télécommande du pilote et le drone, puis intervient sur ce dernier en prenant le contrôle du drone. Elle ordonne ensuite au drone de suivre un itinéraire prédéterminé et d'atterrir en toute sécurité dans un lieu prédéterminé. Cette atténuation chirurgicale peut se produire dans une certaine plage, en fonction de la puissance de sortie nécessaire pour intervenir sur la liaison de communication du drone malveillant.

Cette cyber-prise de contrôle RF est intégrale, ce qui signifie qu'elle passe sans problème de la détection de drones malveillants à la prise de contrôle puis à l'atterrissage en toute sécurité. Il peut également être déployé automatiquement, éliminant ainsi le risque d'erreur humaine.

Contrairement aux autres technologies d'atténuation, la cyber-prise de contrôle RF préserve la continuité en évitant les dommages collatéraux ou les interférences avec d'autres systèmes de communication. Elle peut également faire la distinction entre les drones autorisés et non autorisés, permettant ainsi aux drones autorisés d'une organisation de continuer à opérer pendant la lutte contre les drones malveillants.

Comme elle dépend d'une transmission courte, elle peut également affronter des hordes de drones non autorisés en atténuant rapidement chacun d'eux dans sa propre fréquence et son propre modèle de transmission.

Étant donné que l'atténuation des cyber-prises de contrôle RF ne détruit pas le drone, comme les lasers ou les EMP, les organisations peuvent récolter les fruits de l'intelligence à l'intérieur du drone (conformément aux lois en vigueur, bien entendu).

La cyber-prise de contrôle RF se focalise sur des drones commerciaux spécifiques fabriqués à base de RF ou à monter soi-même et sur le dépassement de leurs protocoles spécifiques.

Considérations d'ordre opérationnel

Les entités autorisées à employer légitimement des technologies de systèmes de lutte contre les avions sans pilote (C-UAS) doivent être conscientes de certaines considérations environnementales qui peuvent avoir une incidence directe sur le fonctionnement de ces technologies. Ces considérations peuvent inclure une visibilité directe limitée, le bruit des radiofréquences (RF) et la propagation des signaux radio.

De plus, l'atténuation d'un drone n'est pas liée aux techniques susmentionnées. L'atténuation peut également s'obtenir en trouvant la localisation de l'opérateur du drone et en le faisant cesser ses opérations. L'intégration de technologies d'atténuation multicouches constitue la stratégie la plus efficace pour accroître la probabilité de contrer une menace donnée.

Pour plus d'informations, nous vous invitons à visiter : www.d-fendsolutions.com