Équipements et systèmes anti-mini drones
Technologies avancées et ciblage intelligent

Dr. Mahmoud Al Maharmah

Chercheur et expert militaire, Ancien délégué du Royaume hachémite de Jordanie à la CIMCT

Il est devenu bien clair que les mini drones constituent l'une des armes les plus importantes que les organisations terroristes cherchent à acquérir et à utiliser dans leurs opérations criminelles. Ces engins se caractérisent par leur prix modéré, la facilité de les manier, la capacité à échapper aux radars, la précision de ciblage et la sauvegarde de la vie humaine. Les drones ne se limitent pas à mener des attaques sophistiquées mais contribuent à l'espionnage, à la collecte d'informations et au trafic de drogue, dont les bénéfices servent à financer ces groupes.

Utilisation accrue

Selon l'indice mondial du terrorisme 2023, le recours aux drones pour lancer des attaques terroristes augmente très rapidement. Le rapport dénombre 65 organisations capables d'utiliser des drones dans leurs opérations, dont Daech, Boko Haram et le groupe Houthi. Le rapport avertit que l'incapacité de prendre des mesures rapides et fortes fait de ces avions une source de grande inquiétude.

À la lumière de ces indicateurs et en l'absence de cadre juridique ou éthique empêchant ces drones d'atteindre les mains d'organisations terroristes, les institutions militaires et sécuritaires se hâtent de développer des contre-systèmes qui détruisent ces drones ou les empêchent d'atteindre leurs objectifs, compte tenu de la difficulté de les voir à l'œil nu ou de les détecter par les radars de défense aérienne - conçus pour détecter les gros avions. Cependant, même si certains systèmes anti-aériens conventionnels sont efficaces contre les mini drones, leur coût élevé – comparé au faible coût d'un drone – complique la question. Ainsi, un seul missile Patriot coûte environ 1 million de dollars, tandis qu'un mini drone coûte moins de 500 dollars.

Toutefois, diverses technologies dites « systèmes de lutte contre les drones » sont développées. Elles utilisent une variété de capteurs pour détecter les composants physiques des drones et les centres de commande qui les contrôlent, tout en

intégrant les données liées à la surveillance, au suivi et à la destruction de la menace ou à sa neutralisation. Ces systèmes permettent également d'avoir une perception globale de l'ampleur de la menace que représentent ces avions et de prendre les décisions appropriées au bon moment.

Étapes de ciblage des «drones»

Le ciblage des drones passe par plusieurs étapes, comme suit:

Etape 1/ Détection: Il s'agit de détecter le drone par le centre de contrôle et de le distinguer d'un avion commercial ou de tout autre objet. Différentes techniques de détection et d'identification sont utilisées, tels que les radars, les scanners radiofréquences (RF), les capteurs acoustiques et les capteurs optiques. Les systèmes radar peuvent détecter les drones et identifier leur taille, leur vitesse et leurs schémas de vol. Les scanners radiofréquences surveillent les fréquences radio utilisées par ces drones pour les communications. Les capteurs acoustiques peuvent détecter les signatures sonores uniques des avions, tandis que les capteurs optiques peuvent les détecter et les suivre visuellement.

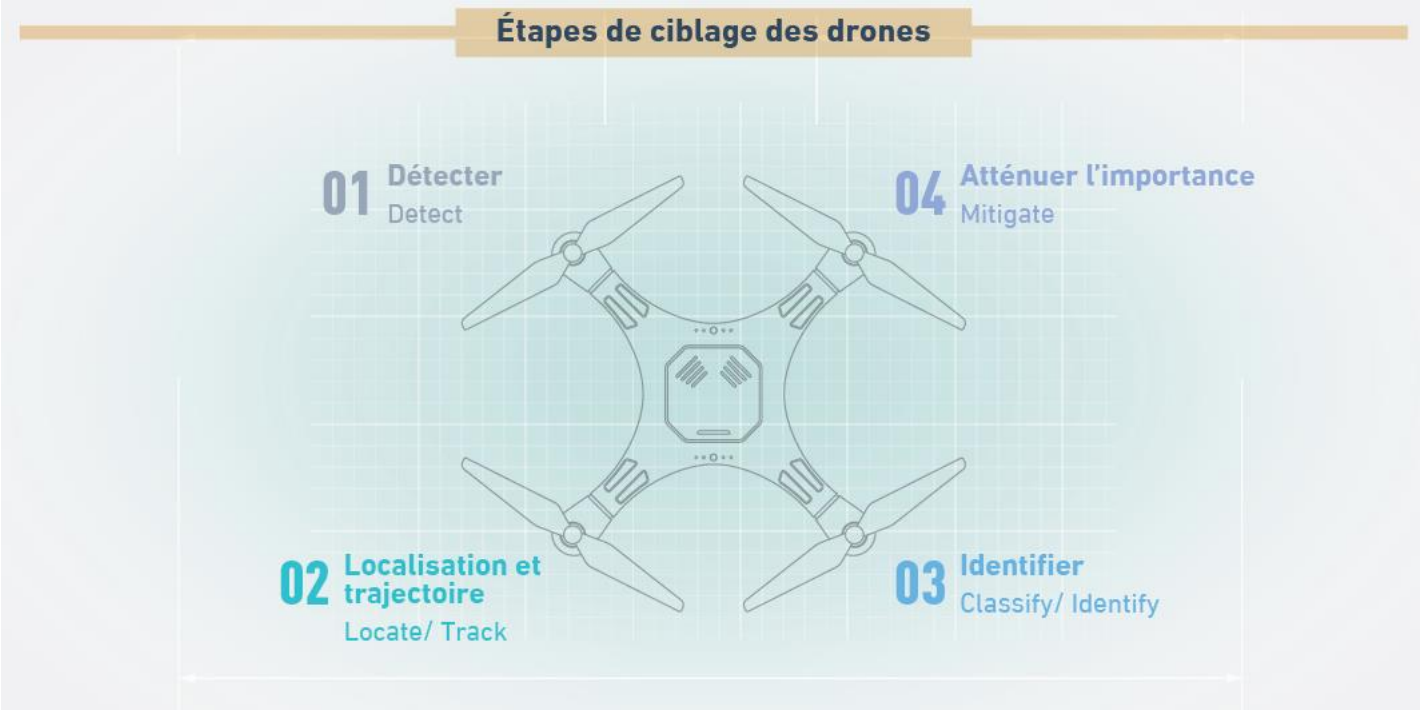
Il convient de noter qu'il n'existe pas de technologie unique capable de détecter et de suivre tous les types de drones en toutes circonstances. Les systèmes électro-optiques ne fonctionnent que de jour, tandis que les systèmes électro-optiques et les systèmes infrarouges, en plus de certains systèmes radiofréquences, nécessitent une ligne de mire directe vers la cible, ce qui signifie qu'il existe des situations dans lesquelles la contre-mesure peut ne pas être capable de détecter et de suivre ces avions.

Etape 2/ Localisation et trajectoire: Il s'agit de déterminer la localisation et la trajectoire de l'avion à un moment précis, ce qui permet au centre de contrôle de le suivre. Une fois qu'un drone est détecté, des systèmes de suivi sont utilisés pour surveiller son emplacement et sa trajectoire. Ces systèmes peuvent utiliser un radar, des caméras ou d'autres capteurs pour suivre le mouvement du drone en temps réel, ce qui permet d'évaluer le niveau de menace et de planifier une réponse appropriée.

Etape 3/ Classification et identification: Cette étape permet de classer l'avion automatiquement ou par l'opérateur du système, déterminer son type, son groupe, son constructeur, son système de communication et le modem de l'engin, et ce par reconnaissance visuelle, prise d'empreintes radiofréquences ou analyse des signaux de communication de l'avion. Connaître l'identité de l'avion permet de déterminer s'il constitue une menace et s'il est exploité légalement ou illégalement.

Quatrième étape: Prévention, neutralisation ou destruction: Un drone intercepteur peut décoller pour s'approcher du drone ennemi, puis lancer son filet pour l'attraper. Ce n'est pas forcément la seule solution pour neutraliser son danger, mais le brouillage radiofréquence peut également lui faire perdre le contact avec son opérateur, le contrôler ou le désactiver à l'aide de réseaux laser.

La figure suivante montre les étapes par lesquelles passent les systèmes anti-drones. Ces étapes peuvent être utilisées comme référence pour comprendre l'étendue de la différence entre les technologies utilisées dans les systèmes anti-drones:



Systèmes et équipements de contre-mesures

Il existe de nombreux systèmes et équipements défensifs utilisés pour affronter les drones, comme suit:

Dispositifs de brouillage radiofréquence: Il s'agit d'appareils fixes ou mobiles pouvant être portés à la main ou placés sur des chariots mobiles. Ils peuvent diriger une grande quantité d'énergie radiofréquence vers le drone, ce qui désactive l'unité de contrôle et la pousse vers quatre scénarios, selon le type et les spécifications du

drone: Le forcer à atterrir de manière contrôlée ou le diriger de manière régulière vers l'endroit d'où il a décollé, ou le faire chuter de manière incontrôlable au sol, ou le faire voler de manière aléatoire et incontrôlable. Ces appareils se sont révélés très efficaces pour abattre des drones, car ils peuvent intercepter les signaux de contrôle des drones, pénétrer dans le logiciel embarqué et déterminer leur emplacement avec une précision allant jusqu'à quelques centimètres, ainsi que l'emplacement du véhicule qu'ils contrôlent dans un rayon de 10 kilomètres, puis le système génère de fortes interférences qui empêchent l'ennemi de contrôler complètement le drone. Il fait chuter l'appareil ou le diriger dans la direction opposée pour frapper celui qui l'a envoyé.

Dispositif d'usurpation d'identité: les dispositifs d'usurpation d'identité GPS envoient un signal au drone cible qui remplace le signal de communication que ce drone utilise pour naviguer, et de cette manière, il trompe le drone sur sa véritable position en modifiant en temps réel les coordonnées GPS de l'avion, pour ensuite prendre le contrôle du GPS et guider l'avion ailleurs. Cependant, les dispositifs d'usurpation d'identité peuvent désactiver par inadvertance d'autres systèmes en dehors de l'avion cible, ce qui constitue un danger pour les systèmes de navigation civils, c'est pourquoi l'utilisation de ces appareils est limitée aux champs de bataille et leur utilisation dans des opérations civiles est déconseillée.

Micro-ondes de haute puissance: Les micro-ondes de haute puissance génèrent une impulsion électromagnétique capable de perturber les appareils électroniques. Les impulsions électromagnétiques interfèrent avec les liaisons radio et désactivent ou détruisent les circuits électroniques des drones (ainsi que tout autre appareil électronique à portée) en raison des tensions électriques et des courants haut voltage créés. Les dispositifs MHP peuvent inclure une antenne pour concentrer les impulsions électromagnétiques dans une direction spécifique, réduisant ainsi les dommages collatéraux potentiels.

Pistolet électromagnétique: C'est un pistolet qui émet des impulsions électromagnétiques qui désactivent le drone. La portée de ce pistolet est de quatre kilomètres.

Canon à filet: Ce canon jette son filet sur le drone stabilisant les pales de l'hélice et paralysant ainsi l'appareil, de trois façons différentes:

- Le canon lance le filet depuis le sol pour paralyser le drone. Ce canon peut être porté à la main, à l'épaule ou monté sur une tour. Sa portée effective est de 300 m.

- Le filet est jeté depuis un autre drone, et ce pour pallier la portée limitée du canon.
- Lancer un filet suspendu à un drone ami sur le drone cible.

Laser à haute énergie: Il s'agit d'un dispositif optique à haute énergie qui produit un faisceau lumineux ou laser hautement focalisé qui détruit le drone en altérant sa structure, son système électronique ou son système de contrôle.

Système de cyber-prise de contrôle: Le système de cyber-prise de contrôle ou cyber-suppression est une technologie relativement nouvelle pour lutter contre les drones. Il détecte les transmissions radiofréquence émanant des drones, déterminent le numéro de série du drone et son emplacement grâce à l'intelligence artificielle. Si le système confirme que ce drone est hostile, il envoie un signal pour l'infiltrer, le contrôler et le diriger vers un endroit sûr.

Recours aux aigles pour abattre les avions: L'armée française a adopté la méthode des oiseaux de proie pour abattre les drones lorsqu'ils pénètrent dans un espace aérien réglementé. Ces aigles peuvent détecter les drones à des milliers de mètres et les désactiver ou les neutraliser.

En conclusion

Avec les multiples capacités de la technologie anti-UAS, ces systèmes ne peuvent pas répondre à toutes les menaces émanant de ces avions, ce qui nécessite de continuer à développer les technologies défensives pour pouvoir prendre le dessus sur les drones et les neutraliser.