Veille Cyber – Drones dans les Zones Stratégiques (2020–2025)

Entre 2020 et 2025, les drones ont révolutionné divers secteurs, notamment la défense, la surveillance et la sécurité civile. Leur agilité et polyvalence en font des outils précieux, mais aussi des menaces potentielles pour la cybersécurité des organisations.

Dans les zones stratégiques, les drones peuvent devenir des vecteurs d'attaques cyber redoutables. Cette veille analyse les principales menaces identifiées, les modes opératoires utilisés, et les solutions de cybersécurité mises en place.

JL par Josselin Lerendu

Cyberespionnage par drone (2021–2024)

Objectifs

Scanner des réseaux Wi-Fi à proximité.

Intercepter du trafic non chiffré.

Identifier des adresses MAC d’appareils connectés.

Des drones civils modifiés

peuvent être utilisés pour mener des campagnes d'espionnage. En embarquant des équipements tels que des antennes Wi-Fi longue portée, des cartes réseau configurées en mode moniteur, voire des mini-ordinateurs (Raspberry Pi), ils deviennent des outils furtifs de captation de données.

Des cas ont été signalés autour d'ambassades, d'entrepôts de données sensibles ou de zones d’entraînement militaires.

Attaques de type Man-in-the-Middle (2022–2025)

Simulation de bornes Wi-Fi

Les drones pirates peuvent simuler des bornes Wi-Fi de confiance à l’aide d’outils comme WiFi Pineapple.

Interception des communications

Une fois la victime connectée, l’attaquant intercepte les communications et enregistre les identifiants.

Injection de code malveillant

Les drones peuvent injecter du code malveillant dans les appareils connectés.

Spoofing et jamming de signaux GPS (2023–2024)

Spoofing

Le drone émet un faux signal GPS plus fort, forçant les récepteurs à se géolocaliser ailleurs.

Jamming

Le drone brouille tous les signaux satellites reçus localement.

En 2024, les Pays-Bas ont alerté sur un pic d’attaques GPS par spoofing dans les couloirs aériens et zones maritimes. Les drones peuvent simuler des signaux satellites pour perturber les systèmes de navigation embarqués.

Injection de malware et attaques réseau (2021–2025)

1

Connexion à un réseau Wi-Fi

Le drone se connecte à un réseau Wi-Fi mal sécurisé.

2

Injection de malware

Le drone injecte un logiciel malveillant dans un appareil connecté.

3

Exploitation de failles

Le drone exploite des failles type SMBv1 ou RDP mal configuré.

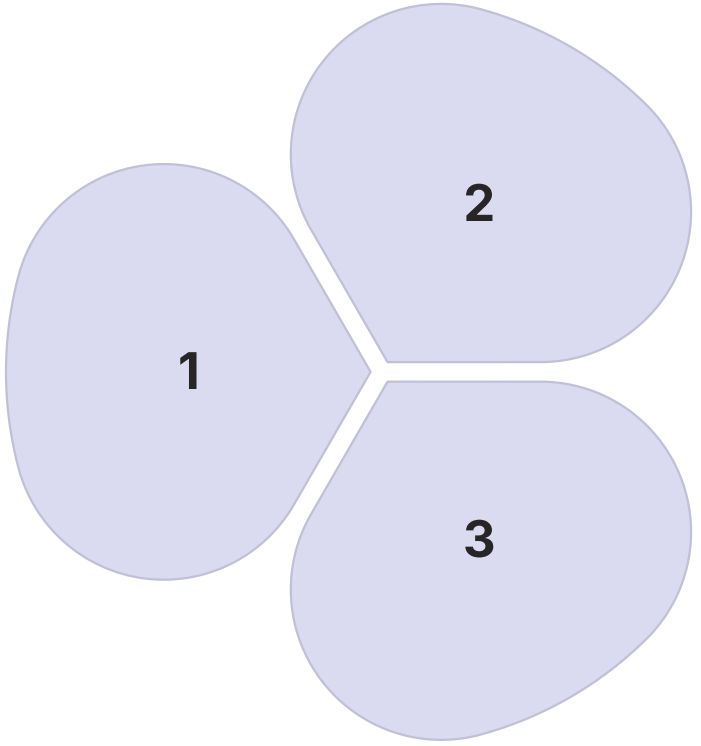
4

Déploiement de ransomwares

Le drone déploie des ransomwares ou vole des données sensibles.

Attaques par DDoS (2022–2025)

Saturation de la bande passante



Interruption des services

Blocage temporaire d’accès

En volant autour d’un bâtiment stratégique, un drone équipé d’un émetteur Wi-Fi peut bombarder un réseau local de requêtes TCP/UDP ou DNS, provoquant saturation de la bande passante, interruption des services et blocage temporaire d’accès pour les utilisateurs.

Technologies d’interception cyber (2022–2025)

Détection et suivi

Radar Doppler pour drones.

Caméras optiques/thermiques avec IA.

Analyse de spectre RF.

Prise de contrôle (takeover)

Capture du signal entre le drone et son opérateur.

Injection d’un faux signal de commande.

Redirection vers une zone sécurisée.

Neutralisation physique

Systèmes PARADE (France).

Armes à micro-ondes (type THOR).

Filets anti-drones.

Conclusion

La prolifération des drones, leur miniaturisation et leur puissance technique les rendent aujourd’hui incontournables… mais aussi dangereux. Dans les zones stratégiques, ils deviennent de potentiels agents d’intrusion cyber capables de capter, injecter ou perturber des infrastructures critiques.

La réponse ne peut pas être uniquement physique : une approche cyber-intelligente, combinant surveillance réseau, détection radio, et anticipation comportementale, est essentielle.

Sources

Drone-Actu – _Les drones et la cybersécurité : comment éviter les failles potentielles_

Sénat – Commission Défense – _Se préparer à la “guerre des drones” : un enjeu stratégique pour la France_

CS Group / Thales – _PARADE : Système français de lutte anti-drone pour la Défense_

France Inter – _Les drones pirates, une menace pour les centrales nucléaires_

Le Monde – _La prolifération des drones : un risque croissant pour la sécurité_