



# Sécurité et cyber-sécurité en robotique aérienne





## Département Technique de Marche

- Les réseaux hétérogènes
- L'enseignement à distance
- La sécurité d'accès
- La sécurité des communications
- L'internet des objets (IoT)
- L'analyse des big data
- Les applications sur systèmes nomades
- L'hébergement des bases de données



## WHAT?

La sécurité anti-drone et/ou la sécurité des drones : nouveaux enjeux pour les entreprises.

Prémunir les entreprises contre les attaques aériennes réalisées depuis un drone.

## WHY ?

Vif succès des drones dans le monde civil auprès du grand public et des professionnels :

1. Technologie alternative aux solutions préexistantes
2. Vecteur de solutions innovantes : les drones sont polyvalents, efficaces et peu onéreux
3. Alliance des hommes et des technologies

## RISQUES ?

La sécurité est aujourd'hui un enjeu majeur pour les systèmes critiques : systèmes à forte exigence de sûreté/sécurité.

Bien que cela ne soit encore jamais arrivé, les gouvernements du monde entier craignent depuis plusieurs années que des drones ne soient utilisés pour réaliser une attaque terroriste.

Un simple drone de loisir peut servir à faire du sabotage industriel

## RISQUES ?

- Prendre le contrôle des drones (livreurs de colis, surveillance...)
- Explosion de l'internet des objets = autant de cibles potentielles
- Voler des données confidentielles et privées
- Prendre le contrôle d'un clavier sans fil
- Interférer dans les commandes d'installations
- Utiliser un brouilleur d'ondes
- Bloquer ou envoyer des transmissions radio
- Perturber voire attaquer des réseaux sans fil de type Wi-Fi
- Provoquer des interférences électromagnétiques
- Pirater à distance
- ...

partout où des hackers ne peuvent mettre physiquement les pieds.

## HOW?

Evaluer les vulnérabilités d'un système et mettre en place une stratégie de défense et/ou de résilience :

- Approche intégrée cyber-sécurité
- Approche intégrée sécurité
- Aspects communication
- Aspects commande
- Assurer la sûreté de fonctionnement
- Prendre en compte les modes de fonctionnement
- Prendre en compte les situations des systèmes
- ...

Merci de votre attention

[alexandre.marchal@henallux.be](mailto:alexandre.marchal@henallux.be)  
[julien.lecointre@henallux.be](mailto:julien.lecointre@henallux.be)