Cybersécurité dans l'espace : quels sont les défis ?

1) La vulnérabilité des satellites

Le déploiement de satellites spatiaux entraîne de nouvelles menaces pour la sécurité.

Des télécommunications satellitaires, passe par l'accès à des connexions internet pour des millions de personnes dans le monde ; les satellites et les services spatiaux qu'ils fournissent sont essentiels à notre fonctionnement en tant que société moderne. Mais la sécurité est une préoccupation constante, qui ne fera qu'augmenter.

Alors que les cybercriminels améliorent leurs capacités, il est possible qu'ils se tournent vers le ciel pour trouver de nouvelles cibles et opportunités.

- **Brouillage et usurpation d'identité**

Le brouillage et l'usurpation visent directement les liens entre les satellites et les stations au sol. Et en brouillant les connexions, le flux d'informations est perturbé. Ce qui peut être crucial en cas de conflit.

Exemple : En effet, cette année, les services internet ViaSat et Starlink en Ukraine ont fait l'objet de brouillage, d'usurpation du GPS et d'autres cyberattaques, et ce dans un contexte d'invasion du pays par la Russie.

- **Pirater les satellites**

Une cyberattaque réussie contre un satellite pourrait avoir des conséquences importantes. En bloquant les communications avec le satellite, on pourrait par exemple interrompre les communications et les services vitaux pour des millions de personnes. Elle pourrait même modifier la trajectoire d'un satellite dans le but de le perturber, voire de l'endommager définitivement.

- **Les satellites ne sont pas construits pour durer éternellement.**

Une fois qu'un satellite a été lancé dans l'espace, il est difficile de mettre à niveau les systèmes informatiques qui l'alimentent. Si une faille de cybersecurité apparaît, elle pourrait être présente pendant toute la durée de vie du satellite. Cela pourrait poser problème si des cyberattaquants trouvaient le moyen de perturber ou d'altérer les services.

Elles peuvent causer des ravages sur les systèmes d'armes stratégiques et compromettre la dissuasion en créant de l'incertitude et de la confusion et d'autres facteurs qui laissent les systèmes satellitaires ouverts aux attaques.

2) L'amélioration des satellites contre les cyberattaques.

Mise en place des fonctionnalités des nouveaux satellites pour renforcer la sécurité :

Cryptage : Les communications satellites doivent être cryptées pour protéger les données contre les interceptions.

Authentification et autorisation : Les systèmes de satellites doivent être équipés de mécanismes d'authentification et d'autorisation pour empêcher les accès non autorisés.

Détection des intrusions : Les satellites doivent être équipés de systèmes de détection des intrusions pour détecter les activités suspectes et les tentatives d'attaques.

Conclusion :

Les gouvernements et les entreprises prennent des mesures pour protéger leurs systèmes spatiaux contre les cyberattaques. En effet, les satellites sont devenus de plus en plus importants pour les communications, la navigation, la surveillance... Avec l'augmentation de l'utilisation des satellites, la vulnérabilité des satellites aux attaques est devenue plus évidente.

Des attaques de plus en plus sophistiquées contre les satellites ont été menées, ce qui a conduit à une prise de conscience de la nécessité de protéger les satellites contre ces cyberattaques. Donc de nouvelles mesures de sécurité et de protection des satellites ont été développées pour réduire leur vulnérabilité aux attaques.