


	Responsable / <i>Responsibile</i> : Ladislav HAJNAL	Ingénieur ENAC Année scolaire 2018/2019
S8 SSI	Mineure « Sécurité des systèmes d'information »	  

OBJECTIFS / OBJECTIVES

A la fin du cours l'étudiant IENAC saura mener une analyse de sécurité et proposer des mécanismes techniques ou non pour améliorer la sécurité d'un système d'information du domaine aéronautique.

L'aviation Civile est un **Opérateur d'Importance Vitale**¹. Ceux-ci sont indispensables au bon fonctionnement du pays et peuvent être des cibles privilégiées aux attaques informatiques qui si elles devaient réussir, pourraient avoir des conséquences très graves.

La lutte contre les menaces malveillantes ciblant les systèmes d'information est une priorité gouvernementale au travers du Livre blanc sur la défense et sécurité nationale 2013 qui identifie l'amplification du risque de cyber-attaques².

Dans l'aviation civile l'utilisation des systèmes informatiques est ancienne mais si la prise en compte de la « *safety* » (protection contre les menaces accidentelles) pour ceux-ci fait partie de la culture aéronautique celle de la « *security* » (protection contre les menaces malveillantes) est plus récente.

Les systèmes d'information ATM par exemple présentent des caractéristiques particulières pouvant susciter l'intérêt d'agents malveillants, et souffrir de vulnérabilités possiblement exploitables en particulier dès lors que le dit système s'ouvre sur le monde. Et comme les systèmes ATM sont amenés à être de plus en plus interconnectés, cela augmente la « surface d'attaque » et les rendent potentiellement sujet à la malveillance.

La prise en compte simultanée des objectifs fonctionnels de sûreté et de sécurité afin d'assurer en toute sécurité l'écoulement du trafic aérien peut cependant être difficile et relève d'une démarche d'ingénierie globale.

¹ La Commission européenne propose la définition suivante: « *les infrastructures critiques sont des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des Etats membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base* ».

² Installée par le chef de l'Etat en juillet 2012, la Commission chargée de l'élaboration du Livre blanc sur la défense et la sécurité nationale a publié son rapport le 29 avril 2013. Le Livre blanc 2013 définit les orientations stratégiques de défense et de sécurité d'ici 2025. Il fonde son analyse sur les évolutions intervenues depuis le précédent Livre blanc (2008) : la crise économique et le renforcement des contraintes budgétaires, le printemps arabe et la multiplication des foyers d'instabilité, la hausse des budgets militaires en Asie (Chine, Corée du Sud, Inde et Japon), **l'amplification du risque de cyber-attaques**.

Aujourd'hui, les enjeux de la sécurité des systèmes d'information sont mieux compris par certains dirigeants qu'auparavant. Avec les incidents qui se multiplient³, l'actualité montre aussi une sensibilité au sujet de plus en plus grande du grand public. Dans le même temps, les outils de la sécurité des systèmes d'information se multiplient au prix parfois d'une complexification technique des systèmes d'information qui les intègrent.

Ce mouvement doit s'accompagner d'une montée en compétence et en expertise des ingénieurs de l'entreprise car la SSI est un domaine majeur pour les ingénieurs.

C'est pourquoi il est essentiel de former nos futurs ingénieurs aux enjeux et aux techniques de sécurité du système d'information.

³ intrusion malveillante sur le réseau du palais présidentiel, vol de secrets industriels, atteintes à la réputation de l'entreprise par voie électronique, usurpations d'identité, atteintes à la vie privée sur les réseaux sociaux....