Organisation de l'aviation civile internationale

HLCAS/2-WP/18
16/10/18

NOTE DE TRAVAIL

DEUXIÈME CONFÉRENCE DE HAUT NIVEAU SUR LA SÛRETÉ DE L'AVIATION (HLCAS/2)

Montréal, 29 et 30 novembre 2018

Point 2 : Stratégies futures de gestion des risques liés à la sûreté de l'aviation

ÉLABORATION D'UNE STRATÉGIE MONDIALE DE CYBERSÉCURITÉ

(Note présentée par la Roumanie)

SOMMAIRE

La présente note contient des recommandations à l'intention des États et de l'industrie, qui devraient appuyer activement l'élaboration d'une stratégie mondiale de cybersécurité dans l'aviation civile.

La suite à donner par la Conférence de haut niveau sur la sûreté de l'aviation figure au paragraphe 4.

1. INTRODUCTION

1.1 Le Sommet Europe, Moyen-Orient et Afrique (EMEA) sur la cybersécurité dans l'aviation civile s'est tenu à Bucarest (Roumanie) du 7 au 9 mai 2018. Il a réuni 416 délégués de 55 États et 19 organisations internationales. Les discussions ont porté sur la manière d'harmoniser et de promouvoir les cadres de cybersécurité.

1.2 Le Sommet a rappelé la *Déclaration de Dubaï sur la cybersûreté en aviation civile*, initialement présentée à Dubaï le 5 avril 2017. En outre, il a reconnu les travaux accomplis par le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC) de l'OACI et ceux qu'il mène actuellement afin d'examiner tous les éléments du cadre aéronautique international qui pourraient être touchés par des cyberincidents.

2. ANALYSE

2.1 Il y a dix ans, la cybersécurité suscitait peu d'intérêt en tant que question internationale dans le secteur aéronautique. À partir du début de la décennie actuelle, les experts en aviation ont signalé qu'une cyberattaque malveillante contre les vols d'aviation civile pourrait être catastrophique. Les modèles de sécurité et de sûreté doivent être adaptés aux changements radicaux amenés par les technologies dans les domaines de la conception, de la production, de l'utilisation et de l'entretien.

2.2 Le cyberespace est devenu un support essentiel d'interactions économiques, sociales et politiques. Mais l'augmentation de l'interdépendance et des perspectives économiques s'est accompagnée de vulnérabilité et d'insécurité. Certains experts estiment que les mégadonnées, l'apprentissage machine et « l'internet des objets » pourraient entraîner une hausse du nombre de connexions internet, qui atteindrait presque le trillion d'ici 2035. Le nombre de cibles potentielles d'attaques, par des acteurs privés et publics, augmentera considérablement et englobera tout, des systèmes de contrôle industriels aux stimulateurs cardiaques, en passant par les voitures autonomes et les drones, et enfin et surtout, l'aviation civile.

2.3 À l'image d'autres secteurs qui se sont engagés dans « la révolution numérique », l'aviation doit préserver la confiance des parties prenantes grâce à la perception précise des vulnérabilités et des possibilités, ainsi que la compréhension des menaces. Un secteur de l'aviation civile connecté et numérisé fait face aux défis suivants :

2.3.1 À mesure que les systèmes et services du secteur aéronautique sont de plus en plus connectés, la surface d'attaque potentielle des systèmes exposée à l'adversaire est de plus en plus étendue et complexe ; la cible est donc plus grande.

2.3.2 Étant donné que le secteur aéronautique dépend beaucoup des technologies, et de plus en plus du cyberenvironnement, une réforme mondiale sera nécessaire pour comprendre et surmonter les différences culturelles entre les deux secteurs. Créer une culture commune, en examinant ensemble les difficultés et les solutions possibles, exigera une coopération interdisciplinaire.

2.3.3 La perception de la menace que représente le pouvoir numérique sera essentielle à la compréhension et à la gestion du risque. Il est nécessaire que tous les membres du secteur parviennent au même niveau de perception et de compréhension afin de faire face au risque potentiel et de promouvoir un dialogue collaboratif qui valorise les points de vue multiples.

2.3.4 Si le secteur aéronautique possède une expérience de plusieurs décennies dans la résolution de questions de sécurité et de sûreté, les défis en matière de cybersécurité sont relativement nouveaux. Il pourrait être plus long pour le secteur de mettre au point et remplacer les systèmes aéronautiques que pour les personnes malveillantes de développer leurs capacités, ce qui complique la réalisation d'évaluations de risque et de modèles de menace précis.

2.3.5 Les investissements dans la gestion du trafic aérien (ATM) portent déjà leurs fruits, mais l'utilisation de technologies de pointe telles que les systèmes mondiaux de localisation (GPS), la communication numérique et la surveillance dépendante automatique en mode diffusion (ADS-B) implique de devoir gérer les vulnérabilités qu'elles apportent et d'encourager la cyberrésilience.

2.3.6 Les aéroports regroupent plusieurs organisations distinctes qui peuvent avoir différentes approches, et la cybervulnérabilité de l'une peut affecter toutes les autres. Il est essentiel de dûment protéger les systèmes de sûreté matériels contre les cybermenaces dans les aéroports.

2.3.7 Les politiques et règlements nationaux et internationaux en matière de sécurité et de sûreté matérielle sont convenus et compris, mais la question de savoir comment la cybersécurité aéronautique peut atteindre le même niveau de maturité et de clarté reste

floue. C'est pourquoi l'OACI, l'AESA, EUROCONTROL et la CEAC, ainsi que d'autres organismes multilatéraux, doivent avancer la main dans la main pour élaborer des politiques et des règlements et développer une pensée systémique cohérente, une gouvernance et une responsabilisation, une confiance solide, et un processus de prise de décision humain sûr au sein d'un cyberenvironnement commun, multifonctionnel et transfrontalier.

2.3.8 L'OACI est bien placée pour rassembler les nombreuses initiatives mondiales en matière de cybersécurité de l'aviation, apporter de la cohérence, jouer un rôle moteur et établir des normes. En vue de promouvoir la cohérence dans l'élaboration de normes relatives à la cybersécurité entre les pays, et d'encourager le dialogue et la collaboration entre les différentes parties prenantes, il est nécessaire de procéder à une évaluation critique des Annexes (8, 10, 17, 18, etc.) de la Convention de Chicago et de les amender du point de vue de la cybersécurité. Il existe un besoin réel de reconnaître que l'intervention illicite par des moyens virtuels est aujourd'hui une réalité, et d'incorporer des perspectives virtuelles avec de nombreux parallèles au point de vue matériel actuel.

2.3.9 Le développement de possibilités en matière de cybersécurité – synergie entre les personnes, les technologies et les processus – en utilisant une approche opérationnelle basée sur un réseau d'information, et des capacités de de détection, de protection, de défense, d'analyse, de décision, de réaction et de rétablissement, garantiront la résilience de l'aviation civile dans l'avenir prévisible.

2.3.10 Le partage exhaustif et opportun des informations réduira les risques au minimum, et la valeur ajoutée d'une telle collaboration est une meilleure gestion de la cybersécurité pour les parties prenantes. L'European Center for Cybersecurity in Aviation, récemment créé en lien avec la CERT-EU, l'Aviation-Information Sharing and Analysis Center ou les centres des opérations de sûreté, sont des multiplicateurs de force pour les États membres en matière de cybersécurité.

2.3.11 Le partage d'informations entre les secteurs civil et militaire est aussi important. L'aviation civile pourrait tirer des leçons de la manière dont le secteur militaire perçoit et aborde le défi de la sécurisation des aéronefs et des systèmes dans des environnements confrontés à des actions de brouillage intentionnel des radiofréquences et de leurrage, et celui des cybermenaces.

2.3.12 L'AESA a publié la « Bucharest Declaration on high-level efforts in civil aviation cybersecurity » (Déclaration de Bucarest sur les efforts de haut niveau en matière de cybersécurité dans l'aviation civile), axée sur plusieurs objectifs, tels que la coordination au niveau européen, la coopération internationale, les évaluations des risques, le renforcement de la sensibilisation, le partage d'informations, et la recherche et le développement. Il y avait aussi une volonté d'harmoniser les règlements à l'échelle internationale car les défis nécessitent une approche holistique plus large.

3. CONCLUSION

3.1 Considérant que pour le développement d'un cycle de vie de la cybersécurité, la gestion des cyberrisques englobe le concept, la conception, l'assurance, la fourniture, la construction, la livraison, l'utilisation et l'entretien, il est nécessaire d'adopter une approche globale, exhaustive et intégrée.

Pour combler l'écart entre la situation actuelle et la situation voulue, il faut agir au plus tôt contre les risques et les menaces dans le nouveau cyberenvironnement.

3.2 Les responsables et les représentants d'États, d'organisations régionales, d'organisation internationales et d'entreprises qui ont participé au Sommet Europe, Moyen-Orient et Afrique sur la cybersécurité dans l'aviation civile, tenu à Bucarest (Roumanie) du 7 au 9 mai 2018, ont examiné les défis que posent les cybermenaces à l'aviation civile internationale.

3.3 Conscients de la nécessité de veiller à la sécurité, à la sûreté et à la continuité de l'aviation civile de façon ordonnée, nous formulons les recommandations suivantes :

3.3.1 Les cadres de cybersécurité des États et de l'industrie devraient être élaborés de la manière la plus harmonisée possible ;

3.3.2 Les États et l'industrie devraient encourager la coopération régionale dans la définition de stratégies communes, ainsi que l'échange d'informations et des meilleures pratiques, suivant l'exemple d'initiatives existantes ;

3.3.3 Des cadres de confiance permettant le partage sécurisé des informations devraient être favorisés, selon qu'il convient ;

3.3.4 Les États et l'industrie devraient collaborer pour déterminer les besoins à long terme en ressources humaines et établir des stratégies pour attirer, former et retenir la prochaine génération de professionnels de l'aviation ;

3.3.5 Les États et l'industrie devraient appuyer activement l'élaboration d'une stratégie mondiale de cybersécurité, sous les auspices de l'Organisation de l'aviation civile internationale.

4. SUITE À DONNER PAR LA CONFÉRENCE

4.1 La Conférence de haut niveau sur la sûreté de l'aviation est invitée à approuver les conclusions et à convenir de la nécessité d'une approche globale, exhaustive et intégrée dans le domaine de la cybersécurité.

— FIN —