Organisation de l'aviation civile internationale

AN-Conf/14-WP/100
28/6/24

NOTE DE TRAVAIL

QUATORZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 26 août – 6 septembre 2024

Point 4: Hyperconnectivité du système de navigation aérienne
4.2 : Cybersécurité et résilience des systèmes d'information

UTILISER DES MÉTHODES AGILES POUR COMBLER LES LACUNES EN MATIÈRE DE POLITIQUE DE CYBERSÉCURITÉ

(Note présentée par les États-Unis)

RÉSUMÉ ANALYTIQUE

La discipline de la cybersécurité a des ramifications transversales qui touchent chaque aspect du système, notamment les personnes, les processus et les technologies. De nouvelles technologies font leur apparition et elles auront un profond effet sur la capacité et l'efficacité de l'aviation civile. Les avantages qu'apportent ces nouvelles technologies exacerbent les défis pour les mécanismes de défense de la cybersécurité puisque les acteurs malveillants tireront parti de ces technologies pour améliorer leurs moyens et leurs méthodes d'attaques. Étant donné la nature de la cybersécurité, des moyens novateurs et plus agiles sont nécessaires pour accélérer la manière dont les éléments indicatifs sur la cybersécurité de l'OACI sont mis à la disposition des États membres de l'OACI et des parties prenantes de l'aviation.

Suite à donner : La Conférence est invitée à approuver la recommandation figurant au paragraphe 3.

1. INTRODUCTION

1.1 L'écosystème de l'aviation est un système opérationnel mondial et unique, composé de systèmes, de services, de processus, de technologies et de personnes qui sont connectés de manière globale pour transporter les passagers et le fret dans de bonnes conditions de sécurité et de sûreté. Les entités qui contribuent à cet écosystème sont décrites dans la **figure 1.**

1.2 La cybersécurité, tout comme la sécurité et la sûreté physique, est une discipline transversale qui englobe tout l'écosystème de l'aviation afin de protéger et de préserver sa capacité de fonctionnement. La cybersécurité va plus loin et offre des protections urgentes pour défendre les systèmes et les services de l'aviation contre des menaces qui sont dynamiques (p. ex., les logiciels malveillants), imprévisibles (p. ex., attaques de jour 0) et dont l'impact peut se répercuter rapidement dans l'ensemble de l'écosystème (p. ex., attaques de déni de service distribué). La **figure 2** montre de quelle manière la cybersécurité est intégrée dans toutes les composantes de l'écosystème de l'aviation. Lorsque toutes ces composantes, y compris la cybersécurité, sont intégrées de manière fluide, la sécurité et l'efficacité sont assurées.

Figure 1. Les composantes des systèmes, des services et des technologies qui forment l'écosystème de l'aviation

1.3 De nouvelles technologies d'avant-garde, comme l'intelligence artificielle (IA) générative, l'informatique quantique et la biométrie, sont en train d'être intégrées dans l'écosystème de l'aviation afin d'améliorer sa capacité et son efficacité. Les menaces en matière de cybersécurité dirigées contre les systèmes et les services de l'aviation évoluent elles aussi et s'adaptent pour tirer parti des nouvelles technologies afin de développer des moyens plus perfectionnés et susceptibles de causer des dommages à l'infrastructure essentielles et aux données de propriété industrielle. Les acteurs malveillants élargissent aussi les perspectives en utilisant les technologies émergentes pour développer de nouveaux moyens d'exploiter les anciennes vulnérabilités que l'on pensait avoir atténuées il y a longtemps.

1.4 Compte tenu des menaces qui concernent en premier lieu l'écosystème de l'aviation et de la vitesse à laquelle les nouvelles technologies apparaissent et augmentent les risques intrinsèques, la rapidité à laquelle les éléments indicatifs sont élaborés et mis à la disposition des États membres de l'OACI et des parties prenantes de l'aviation est plus importante que jamais.

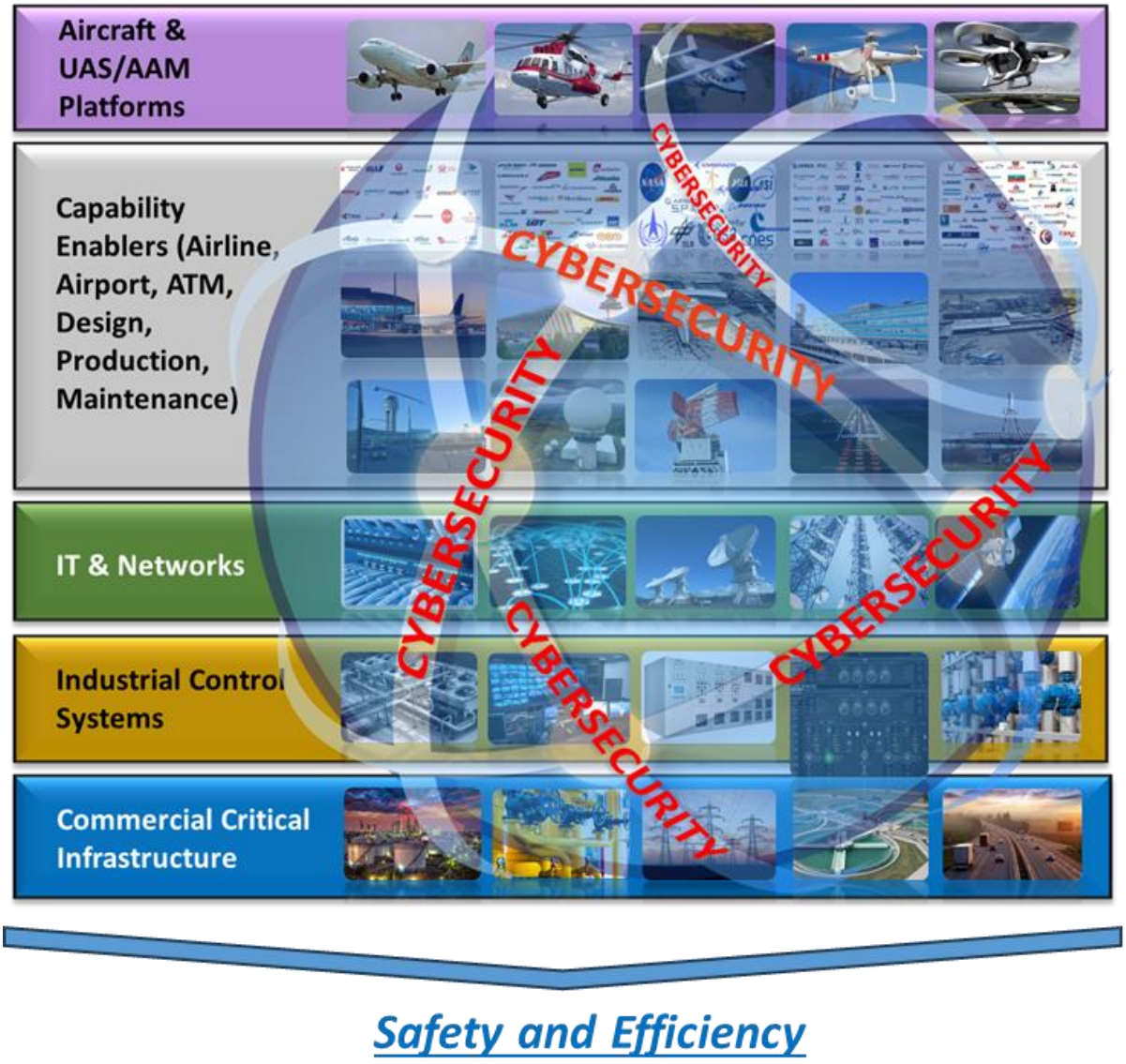

Figure 2. Protections en matière de cybersécurité intégrées dans l'ensemble de l'écosystème de l'aviation

2. ANALYSE

2.1 La cybersécurité est un instrument d'habilitation des principales fonctions de l'aviation (p. ex., communication, navigation et surveillance) et est composé d'un ensemble d'infrastructure, de systèmes et de service d'entreprise qui constituent une barrière de protections contre les menaces locales, régionales et/ou mondiales. Ces menaces évoluent rapidement du point de vue de leur degré de perfectionnement, leur pouvoir de destruction et leur capacité de faire du mal à tout moment et n'importe où dans l'écosystème.

2.2 Les technologies émergentes comme l'IA générative, l'informatique quantique et la biométrie ainsi que d'autres, créent aussi des occasions uniques pour les acteurs malveillants de tirer parti de méthodes et de moyens plus sophistiqués afin de perturber les systèmes et les données de l'aviation civile, en imposant de nouveaux défis aux parties prenantes de l'aviation, aux États membres de l'OACI

et aux instances de réglementation de l'aviation civile pour ce qui est la mise en place de contre-mesures destinées à améliorer constamment leurs protections.

2.3 La croissance rapide des nouvelles menaces exige d'appliquer des stratégies encore plus novatrices et opportunes à l'élaboration et à la mise à disposition d'éléments indicatifs sur la cybersécurité pour les parties prenantes de l'aviation et les États membres de l'OACI afin d'assurer la protection et la résilience de notre écosystème de l'aviation.

2.4 Des initiatives comme la procédure de soumission directe de l'OACI tiennent compte de la nécessité d'accélérer la publication des documents, mais leur champ d'application est limité aux entités qui traitent de sujets ayant un rapport avec les objectifs stratégiques de l'OACI : sécurité et capacité et efficacité de la navigation aérienne. Des éléments indicatifs visant à renforcer la position de l'écosystème de l'aviation du point de vue de la cybersécurité doivent être élaborés et communiqués à l'aide de processus plus agiles et plus opportuns tout en maintenant la qualité et le contrôle de la configuration.

2.5 Compte tenu de ce qui précède, l'OACI est invitée à étudier des moyens et des méthodes d'accélérer l'élaboration, l'examen, la publication et la distribution des éléments indicatifs sur la cybersécurité pour les parties prenantes de l'aviation et les États membres de l'OACI, qui soient proportionnels aux besoins en matière de cybersécurité.

3. CONCLUSION

3.1 La Conférence est invitée à accepter les recommandations qui suivent :

Recommandation 4.2/x — Évaluer la viabilité d'adopter les principes de la méthode Agile

Il est recommandé que l'OACI :

a) prenne conscience qu'il faut adopter des stratégies opportunes, pertinentes et concrètes relativement aux éléments indicatifs sur la cybersécurité afin de les mettre à la disposition des États membres de l'OACI et des parties prenantes de l'aviation ;

b) étudie des moyens et des méthodes d'accélérer l'élaboration, l'examen, la publication et la distribution des éléments indicatifs sur la cybersécurité pour les parties prenantes de l'aviation et les États membres de l'OACI, qui soient proportionnels aux besoins en matière de cybersécurité.

— FIN —