Organisation de l'aviation civile internationale

A42-WP/165[1]
EX/83
24/7/25

NOTE DE TRAVAIL

ASSEMBLÉE — 42e SESSION

COMITÉ EXÉCUTIF

Point 13 : Politique de sûreté de l'aviation

RENFORCEMENT DE LA GOUVERNANCE ET DE LA GESTION DES MENACES NUMÉRIQUES ET DE CYBERSÉCURITÉ PESANT SUR L'AVIATION CIVILE

[Note présentée par le Conseil international de coordination des associations d'industries aérospatiales (ICCAIA) et la Fédération internationale des associations de pilotes de ligne (IFALPA)]

RÉSUMÉ ANALYTIQUE

Le secteur de l'aviation civile dépend de plus en plus de technologies et de systèmes numériques interconnectés, notamment ceux qui régissent ou influencent directement les processus physiques et opérationnels. Si ces technologies apportent des avantages considérables, elles exposent également le secteur à des menaces numériques intentionnelles, involontaires et naturelles, ainsi qu'à des vulnérabilités susceptibles d'amplifier ces menaces et de mettre en danger des opérations critiques.

La plupart des cadres de l'OACI, qu'ils concernent la sécurité, la sûreté ou les opérations, n'ont pas été conçus à l'origine pour faire face à la nature systémique et transversale des menaces numériques, qui s'étendent désormais aux capacités numériques émergentes et aux interdépendances. La faille la plus préoccupante concerne les actes intentionnels et malveillants situés à la frontière entre sûreté et sécurité.

Le présent document invite l'OACI à établir dans un premier temps un cadre interne coordonné de gouvernance et de gestion des menaces numériques qui aligne ses domaines de sécurité, de sûreté et d'exploitation, en mettant l'accent initial sur les menaces intentionnelles et malveillantes. À titre complémentaire, il encourage l'OACI à accélérer l'élaboration des directives et des normes mondiales nécessaires pour atteindre un niveau de performance en matière de sûreté cohérent et efficace dans l'ensemble de l'écosystème aéronautique.

Suite à donner : L'Assemblée est invitée à :

a) reconnaître que toutes les catégories de menaces numériques, qu'elles soient intentionnelles, non intentionnelles ou naturelles, présentent des risques pour l'aviation civile et doivent être traitées dans le cadre d'une approche globale de gouvernance. Celle-ci doit d'abord être mise en place au sein de l'OACI afin de garantir la cohérence et un soutien efficace aux États et au secteur ;
b) demander au Conseil de l'OACI d'entamer la mise en place d'un cadre de gouvernance interne multidomaine et multidisciplinaire pour les menaces numériques au sein même de l'OACI ;

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par l'ICCAIA et l'IFALPA.

c) encourager l'OACI à accélérer l'élaboration de directives et, le cas échéant, de normes et de pratiques recommandées (SARP) afin d'établir une base de référence systémique, harmonisée et adaptative en matière de sûreté numérique pour tous les États et toutes les parties prenantes ; d) recommander à l'OACI de renforcer la sensibilisation et la communication sur le traitement coordonné des menaces numériques par le biais de ses réseaux régionaux, afin de soutenir une action harmonisée et des performances de sûreté efficaces à l'échelle mondiale.	
Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Chaque vol est sûr et sécurisé*.
Incidences financières :	Aucune
Références :	A41-19 Cybersécurité de l'aviation civile, Annexe 17 (*Sûreté de l'aviation*) Annexe 19 (*Gestion de la sécurité*)

1. INTRODUCTION

1.1 La transformation numérique a amélioré les performances de l'aviation civile, mais cette plus grande dépendance au numérique révèle et crée des vulnérabilités liées à l'interconnectivité croissante et à la complexité systémique.

1.2 Cette évolution engendre des défis organisationnels et de gouvernance dus au partage des responsabilités entre les différents domaines de l'OACI, notamment la sécurité, la sûreté, la capacité et l'efficacité, ce qui illustre la nécessité plus large d'une gouvernance holistique et coordonnée.

1.3 Parmi les différentes catégories de menaces numériques, les actes intentionnels et malveillants (communément appelées « cyberattaques ») sont particulièrement urgents à traiter en raison de leur potentiel de perturbation des systèmes critiques de l'aviation et de l'incertitude actuelle quant aux attributions dans les domaines de la sécurité et de la sûreté.

1.4 Cette évolution met également en lumière l'absence d'un cadre mondial apte à mettre en œuvre de manière systématique une approche fondée sur la « sûreté dès la conception » (security by design) et tenant compte des menaces, au moyen de directives et de normes spécifiques à tous les domaines. En l'absence d'approches harmonisées, des mécanismes de coordination provisoires pourraient se révéler nécessaires pour soutenir une action rapide, en particulier dans les contextes opérationnels à haut risque.

1.5 Les menaces numériques, définies comme tout événement préjudiciable potentiel ou réel provenant de capacités numériques ou facilité par celles-ci, ont commencé à retenir l'attention des groupes d'experts et des groupes de travail de l'OACI. Cependant, bon nombre de ces menaces ne sont pas encore suffisamment prises en compte, en particulier lorsqu'elles ne correspondent pas aux définitions classiques d'intervention illicite ou de danger pour la sécurité. Cela est particulièrement vrai pour les menaces intentionnelles et malveillantes qui se situent à la croisée des domaines de compétence de l'OACI, engendrant une incertitude quant à la responsabilité, la surveillance et la coordination des mesures à prendre.

2. ANALYSE

2.1 Les menaces numériques qui pèsent sur l'aviation civile englobent un large éventail d'événements. Ces menaces peuvent être intentionnelles (malveillantes ou non), non intentionnelles (erreur humaine, mauvaise configuration) ou naturelles (phénomènes environnementaux). Elles peuvent provenir de vecteurs numériques, physiques ou hybrides et affecter à la fois les éléments numériques et les systèmes physiques qui en dépendent, compromettant ainsi la sécurité, la sûreté et la continuité opérationnelle de l'aviation. Comprendre ces grandes catégories n'est qu'une première étape ; le secteur doit également se pencher sur la manière dont la transformation numérique en cours amplifie leur complexité.

2.2 La transformation numérique remodèle l'écosystème aéronautique en introduisant non seulement de nouvelles technologies, mais aussi de nouveaux modes de défaillance, d'exposition et de dépendance. Bon nombre de ces risques ne sont pas suffisamment pris en compte par les cadres traditionnels de l'OACI, à commencer par ceux liés à la sécurité et à la sûreté, sans s'y limiter. En l'absence de structure mondiale, les réponses sont inégales, les responsabilités fragmentées et la compréhension commune fait défaut ; autant de conditions qui compromettent la protection et la résilience.

2.3 Au-delà d'une exposition accrue aux actes malveillants, la transformation numérique introduit des complexités structurelles qui remettent en question les cadres existants de gouvernance et de gestion des risques/événements. Elle crée des interdépendances opaques entre les technologies de l'information (TI) et les technologies opérationnelles (TO), des vulnérabilités dans la chaîne d'approvisionnement et un rythme de changement qui dépasse les cycles de certification. L'avionique traditionnelle dépend désormais du cloud, de l'intelligence artificielle (IA) et des liaisons IP (Internet Protocol) dont les composants tiers sont mis à jour chaque mois, ce qui introduit des vulnérabilités qui échappent aux contrôles traditionnels. Les innovations se succèdent à un rythme effréné, tandis que la réglementation évolue lentement, rendant les mesures d'atténuation obsolètes et creusant les disparités entre les États. Faute d'une taxonomie commune et d'un mécanisme de partage des incidents, la communauté ne perçoit que des fragments du problème, ce qui retarde la mise en place de mesures de protection proportionnées.

2.4 L'absence de directives mondiales spécifiques et de SARP fondées sur une philosophie de « sûreté dès la conception » et tenant compte des menaces signifie qu'il n'existe pas d'approche harmonisée et systémique pour lutter contre les menaces numériques dans tous les domaines. Cette absence de référentiel commun de performance pour les États crée un contexte systémique vulnérable, propice à l'émergence de menaces délibérément conçues pour exploiter cette complexité.

2.5 Dans ce contexte, les menaces intentionnelles et malveillantes méritent une attention particulière. Souvent complexes, dynamiques et difficiles à attribuer, ces menaces sont conçues pour exploiter les dépendances numériques afin de provoquer une dégradation ou une perturbation des opérations. Leurs caractéristiques uniques peuvent les placer dans, au-delà ou en dehors des classifications traditionnelles de l'aviation, ce qui rend leur détection, leur signalement et leur traitement difficiles.

2.6 L'expérience opérationnelle montre que certaines interférences numériques malveillantes ne relèvent pas clairement des cadres existants. Un exemple notable est l'usurpation intentionnelle de signaux GNSS, qui consiste à diffuser de faux signaux de positionnement induisant en erreur les systèmes de navigation d'un aéronef sans nécessiter d'accès physique ou d'intrusion visible. Bien qu'intentionnelles et susceptibles d'affecter directement les opérations de vol, ces actions peuvent ne pas répondre aux critères d'intervention illicite définis à l'annexe 17, ni déclencher un rapport obligatoire sur les événements de sécurité en vertu de l'annexe 19.

2.7 Cet angle mort réglementaire limite non seulement la connaissance de la situation et la coordination des réponses, mais surtout, elle démontre la nécessité impérieuse d'un cadre de gouvernance et de gestion qui intègre ces nouvelles formes d'interférences numériques, établisse des seuils de notification clairs et définisse sans ambiguïté les rôles institutionnels entre les domaines de la sécurité et de la sûreté.

2.8 À défaut d'un cadre international coordonné, les États et les autorités régionales ont commencé à adopter diverses approches réglementaires. Cette divergence croissante introduit une complexité pour les acteurs du secteur aéronautique, notamment les constructeurs (OEM), les fournisseurs et les prestataires de services, qui doivent naviguer dans des environnements de conformité hétérogènes. Ce défi requiert une double approche :

- Une stratégie globale et holistique capable de couvrir tout l'éventail des menaces numériques, qu'elles soient intentionnelles, non intentionnelles ou naturelles.
- Un effort ciblé et prioritaire sur les menaces intentionnelles et malveillantes, compte tenu de leur urgence, de leur gravité potentielle et du défaut de coordination réglementaire actuel.

3. CONCLUSION

3.1 Il est essentiel de renforcer la protection contre les menaces numériques pour maintenir la sécurité, la sûreté, la capacité et l'efficacité de l'aviation civile. À mesure que les dépendances numériques s'accroissent dans tous les systèmes et domaines, il devient également nécessaire de mettre en place une gouvernance coordonnée et prospective.

3.2 Pour relever ce défi, l'OACI et ses parties prenantes doivent poursuivre un double objectif clair :

- Adopter une approche holistique qui couvre tout l'éventail des menaces numériques, qu'elles soient intentionnelles, non intentionnelles ou naturelles.
- Donner la priorité au traitement des menaces intentionnelles et malveillantes, qui présentent actuellement le plus grand degré d'incertitude dans la répartition des rôles et la coordination entre les domaines de compétence de l'OACI.

3.3 En favorisant l'harmonisation entre les domaines, en faisant progresser les instruments provisoires et en établissant une compréhension commune, l'OACI peut jouer un rôle central pour garantir une réponse cohérente, adaptative et globalement uniforme face aux risques numériques en constante évolution.

3.4 Cet effort pourrait être chapeauté par le Comité ad hoc de coordination de la cybersécurité (AHCCC) existant, en lui attribuant un mandat spécifique en matière de gouvernance, rôle qu'il ne remplit pas actuellement.

— FIN —