Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/105[1]
TE/33
30/7/19

ASSEMBLÉE — 40e SESSION

COMMISSION TECHNIQUE

Point 30 : Autres questions à examiner par la Commission technique

PERMETTRE L'AVIATION NUMÉRIQUE GRÂCE AU CYBER-DÉVELOPPEMENT DU PERSONNEL ÉLECTRONICIENS EN SÉCURITÉ DE LA CIRCULATION AÉRIENNE (ATSEP)

[Note présentée par la Fédération internationale des associations des électroniciens en sécurité de la circulation aérien (IFATSEA)]

RÉSUMÉ ANALYTIQUE

La prochaine génération de personnel opérationnel, d'équipages et de contrôleurs de la circulation aérienne (ATCO), comptera de plus en plus sur la capacité technique et de gestion des ATSEP pour faire face aux menaces informatiques des systèmes d'information et des infrastructures de communications, navigation et surveillance (CNS) qui protègent le public voyageur. L'obligation incombant aux États d'identifier les infrastructures critiques et de constituer une équipe informatique d'intervention d'urgence se superpose à la responsabilité personnelle des ATCO et de l'ATSEP. Il existe également des chevauchements entre les infrastructures critiques. En cas d'atteinte aux infrastructures plus vastes prenant en charge la gestion du trafic aérien (ATM), la sécurité ATSEP a clairement un rôle à jouer dans la coordination de la reprise tout en veillant à la sécurité des opérations de l'ATM.

Suite à donner : L'IFATSEA invite l'Assemblée à prendre note des informations contenues dans le présent document de travail et demande au Conseil de prendre les mesures nécessaires pour développer un nouveau volet ATSEP sur la sûreté, la sécurité et la cybersécurité, ainsi que la formation correspondante.

Objectifs stratégiques :	Le présent document de travail concerne les objectifs stratégiques en matière de sécurité, de capacité de la navigation aérienne et d'efficacité, ainsi que de sécurité et de facilitation.
Incidences financières :	Le coût de la mise en œuvre d'un nouveau flux ATSEP devrait être minime puisqu'il a simplement élargi la mise en œuvre actuelle de la formation axée sur les compétences décrite dans le Doc 10057.
Références :	Annexe 10 — *Télécommunications aéronautiques*, Volumes I, II, III et IV Doc 8071, *Manuel sur la vérification des aides radio à la navigation* Doc 9683, *Manuel d'instruction sur les facteurs humains*

[1] Versions française, anglaise, arabe, chinoise, espagnole et russe fournies par IFATSEA.

	Doc 9868, *Procédures pour les services de navigation aérienne — Formation* (PANS-TRG) Doc 10057, *Manuel sur la formation et l'évaluation fondées sur les compétences à l'intention des électroniciens en sécurité de la circulation aérienne*

1. INTRODUCTION

1.1 Dans le monde entier, il est prévu de développer de nouvelles infrastructures prenant en charge la gestion du trafic aérien ; y compris, sans toutefois s'y limiter, le système de transport aérien de la prochaine génération (NextGen) et le Programme de recherche ATM dans le cadre du Ciel unique européen (SESAR). Ces visions reposent toutes sur des méthodes de traitement et de communication numériques hautement fiables. Le développement sûr et réussi de ces infrastructures vastes et complexes pose de nombreux défis, notamment la nécessité d'intégrer les nouvelles technologies aux systèmes existants. Ces systèmes ATM interopérables numériques à la pointe de la technologie reposent sur la cybersécurité ; afin de garantir l'intégrité et la sécurité des opérations de trafic aérien. À son tour, cela nécessite du personnel électroniciens en sécurité de la circulation aérienne (ATSEP) doté d'un nouvel ensemble de compétences en évolution. Il est clair que la nature des cybermenaces pour l'aviation changera avec le temps. Cette soumission propose une approche pratique et systématique du développement de la formation, de la pédagogie et des compétences permettant à une nouvelle génération de personnel capable de concrétiser notre vision partagée de l'aviation numérique.

2. DISCUSSION

Sûreté et sécurité dans ATM/ANS

2.1 Les nouvelles réglementations (US PPD-21, EU 2016/1148) obligent de plus en plus les États à définir leurs infrastructures critiques et à identifier les interdépendances croissantes qui les séparent, par exemple entre les télécommunications numériques et les systèmes de gestion du trafic aérien.

2.2 À l'heure actuelle, de nombreux fournisseurs de services de navigation aérienne (ANSP) manquent d'expertise en cyber ; cela est naturel étant donné que, dans le passé, les niveaux de menace étaient très faibles. Ils manquent souvent de personnel qualifié. De nombreux ANSP ont résolu ce problème en recrutant des consultants externes en cybersécurité. Les contrats sont souvent attribués à des entreprises extérieures au secteur de l'aviation, sans grand souci des connaissances du domaine nécessaires pour assurer la sécurité et la réussite des opérations. Il peut être difficile pour des consultants externes de convaincre les ATCO de la menace potentielle pour les opérations de logiciels malveillants qui traversent le « vide » pour des systèmes isolés de l'Internet public. Par conséquent, les entreprises externes ont souvent un effet très limité sur la résilience de nombreux États membres. De plus, le développement d'une culture de sécurité forte, comme la sécurité, est plus efficace lorsqu'il est libéré en interne. Au sein du fournisseur des services de la circulation aérienne (ATS), les sociétés externes n'ont aucune influence sur ATSEP, responsable des systèmes techniques, et sur ATCO, qui dépendent des systèmes pour fournir le service de trafic aérien.

2.3 ATSEP joue un rôle de plus en plus important dans la protection de ces interfaces critiques (A39-WP17 EX/5 de l'OACI). Par exemple, la plupart des pays ont mis en place ou commencent à mettre en place des équipes d'intervention d'urgence informatique (CERT), qui relèvent de

la responsabilité des ATCO et de l'ATSEP. Cependant, le traitement de la cybersécurité dans la formation d'ATSEP est, au mieux, incohérent et, au pire, ad hoc.

Contexte politique et réglementaire

2.4 L'importance de ces questions a été reconnue et inscrite dans un certain nombre d'instruments. Il s'agit notamment des aspects des services réseau d'entreprise de la Federal Aviation Administration (FAA) (FENS), ainsi que du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 établissant des règles communes dans le domaine de la sûreté de l'aviation civile. Dans d'autres régions du monde, les pays risquent de prendre encore plus de retard en matière de cybersécurité. Il est nécessaire de mieux définir les mesures appropriées pour protéger notre avenir commun dans les infrastructures d'aviation numérique, en particulier lorsque le règlement n° 1254/2009 permet aux États membres de déroger aux normes de base communes en matière de sûreté de l'aviation civile et d'adopter des mesures de sûreté alternatives. La Secrétaire générale de l'OACI, M^{me} Fang Liu, a également souligné l'importance d'une telle vision lors du Forum OACI-EASA, le 21 septembre 2018.

3. CONCLUSION

3.1 Proposition d'un volet ATSEP sur la sécurité, la sûreté et la cybersécurité et la formation correspondante.

3.2 Nous suggérons de créer un nouveau flux ATSEP sur la sécurité, la sûreté et la cybersécurité, dans le but de tirer parti de leurs connaissances actuelles des infrastructures aéronautiques avec une base solide pour les menaces et les moyens de défense de ces infrastructures. Nous envisageons une compétence qui s'étend aux zones de chevauchement d'autres infrastructures critiques ; Cela augmentera la résilience de l'aviation, qui s'appuie sur des chaînes d'approvisionnement étendues utilisant des technologies numériques largement répandues sur le marché de masse, bien connues des pirates informatiques et des agences gouvernementales.

3.3 Nous soulevons ce problème parce que différents États membres adoptent des approches radicalement différentes en matière d'ingénierie de la cybersécurité dans les opérations ATM ; Cependant, nous comptons tous sur la force de notre voisin pour maintenir les réseaux de transport. Par conséquent, pour permettre et améliorer la mise en œuvre de la numérisation au niveau mondial dans les systèmes ATM/ATS, nous soulignons l'importance d'une approche commune.

3.4 En outre, l'IFATSEA propose de mettre en place un nouveau circuit de formation en cybersécurité dans lequel les qualifications de premier niveau devraient être définies en coopération avec les États ou les fournisseurs de services de navigation aérienne, tout en ayant pour objectif commun de renforcer la confiance en la résilience des infrastructures aéronautiques de nos voisins défendu par bien qualifié ATSEP.

3.5 En outre, IFATSEA propose à l'OACI de fournir une assistance pour les questions relatives à la formation d'ATSEP, à la mise en œuvre et à l'exploitation de systèmes et de fonctions techniques.

— FIN —