Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A41-WP/122[1]
TE/37
1/8/22

ASSEMBLÉE — 41e SESSION

COMMISSION TECHNIQUE

Point 31 : Sécurité de l'aviation et normalisation de la navigation aérienne

METTRE À JOUR LES OBJECTIFS DE FORMATION EN CYBERSÉCURITÉ EXISTANTS POUR LES ÉLECTRONICIENS EN SÉCURITÉ DE LA CIRCULATION AÉRIENNE (ATSEP) ET DÉVELOPPER DE NOUVEAUX OBJECTIFS DE FORMATION EN CYBERSÉCURITÉ POUR LES ATSEP

(Note présentée par l'International Federation of Air Traffic Safety Electronics Associations)

RÉSUMÉ ANALYTIQUE

Le présent document décrit une proposition visant à mettre à jour les objectifs existants de formation en cybersécurité des électroniciens en sécurité de la circulation aérienne (ATSEP) et à élaborer de nouveaux objectifs de formation en cybersécurité dans le *Manuel de l'OACI sur la formation et l'évaluation fondées sur la compétence à l'intention des électroniciens en sécurité de la circulation aérienne* (Doc 10057).

Suite à donner : L'Assemblée est invitée à :

a) noter les rôles et responsabilités croissants de l'ATSEP dans le cadre de la cyberdéfense aux interfaces avec les domaines de responsabilité adjacents et les nouvelles architectures et modèles commerciaux ATM ;
b) noter la nature dynamique et en constante évolution des cybermenaces ;
c) établir l'ordre de priorité et prendre toutes les mesures nécessaires dans le cadre des *Procédures pour les services de navigation aérienne — Formation* (PANS-TRG, Doc 9868) pour mettre à jour les objectifs de formation en cybersécurité existants et élaborer de nouveaux objectifs de formation en cybersécurité ATSEP pour les objectifs de formation de base et de qualification dans le Doc 10057, Annexe B.

Objectifs stratégiques :	Le présent document de travail porte sur les objectifs stratégiques Sécurité, Capacité et efficacité de la navigation aérienne, Sûreté et facilitation.
Incidences financières :	Il y aura un certain coût associé à la mise à jour et à l'élaboration des objectifs de formation en cybersécurité dans le Doc 10057. Les unités de formation responsables de la formation de base et de qualification ATSEP peuvent être amenées à adapter le contenu des cours de formation pour intégrer les objectifs actualisés ou nouveaux.

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

Références:	A39-WP/370, *Une approche architecturale de cybersécurité pour les systèmes CNS/ATM basés sur " legacy - and swim-base "* Annexe 10 — *Télécommunications aéronautiques*, volumes I, II, III et IV Doc 10057, *Manuel sur la formation et l'évaluation fondées sur la compétence à l'intention des électroniciens en sécurité de la circulation aérienne* Doc 9868, *Procédures pour les services de navigation aérienne — Formation (PANS- TRG)*

1. INTRODUCTION

1.1 Les systèmes CNS/ATM subissent un changement de paradigme avec la mise en œuvre de nouvelles technologies, concepts et modèles d'affaires. Le modèle ANS intégré va être remplacé par une architecture orientée services (SOA) qui est distribuée dans la nature, et les informations sont échangées sur des réseaux tels que SWIM. Systèmes de navigation aérienne. Les services existeront sur le terrain et dans l'espace et même le traitement des données ATM peut se faire sur des systèmes déployés dans des architectures distribuées et géographiquement séparées (par exemple, les ADSP européens et les centres virtuels). Les configurations de systèmes CNS hybrides entrent rapidement en service dans l'ensemble de l'écosystème aéronautique. Si les interfaces d'interconnexion du système de transport aérien entre les intervenants ne sont pas traitées adéquatement en termes de cybersécurité, des vulnérabilités peuvent survenir dans un système ou un élément d'un système chez un intervenant. Bien que ces vulnérabilités ne posent pas de risque majeur pour ce système lui-même, elles peuvent facilement dégénérer en une menace qui pose un risque pour le système d'une autre partie prenante avec des conséquences négatives. La création d'une couche de données ATM entre les parties prenantes du SNA et les parties prenantes externes est nécessaire.

1.2 L'OACI dans la Stratégie de cybersécurité de l'aviation, octobre 2019 Chapitre 7. Le renforcement des capacités, la formation et la culture de la cybersécurité stipulent que « *des formations appropriées liées* à *l'emploi devraient être dispensées en permanence pour soutenir le personnel dans ses rôles quotidiens* » et que « *la cybersécurité pourrait être incluse dans la stratégie pour la prochaine génération de professionnels de l'aviation, car l'OACI est bien placée pour travailler avec les États et l'industrie afin d'élaborer des exigences de compétences fondées sur les rôles pour les professionnels de l'aviation* ». Ainsi, dans le projet de rapport A40-WP/577 de l'OACI, paragraphe 30.36, il est indiqué « *que des orientations spécifiques sur la formation à la cybersécurité pourraient être envisagées pour les futures mises à jour du Doc 10057* ».

1.3 Les ATSEP sont les premiers spécialistes au sein d'un ANSP à aborder tactiquement la cybersécurité à partir de vecteurs d'attaque, soit en réseau, soit en combinaison avec un signal dans l'espace. Ils sont chargés dans ce cas de faire la distinction entre les défaillances techniques et les cyberattaques. Une chose que ces services ont en commun est l'autorisation mettre en service et mettre hors service le matériel et les logiciels par ATSEP. Pour mieux sécuriser le système fonctionnel ATM tel que décrit ci-dessus, ces spécialistes appropriés qui ont également un accès légal aux systèmes techniques ATM/ANS devraient être déployés aux interfaces.

1.4 Les ATSEP jouent un rôle de plus en plus important dans la protection de ces interfaces critiques (OACI A39-WP/17-EX/5). Par exemple, la plupart des pays ont mis sur pied ou commencent à mettre sur pied des équipes d'intervention en cas d'urgence informatique (CERT), qui relèvent de la responsabilité de l'ATSEP. Cependant, la formation de l'ATSEP contenue dans la version actuelle du Doc 10057 de l'OACI est principalement traitée comme des exigences de sécurité, tandis que la référence à la cybersécurité, en particulier pour faire face aux changements de paradigme apportés par SESAR et NextGen, y compris la vision CANSO ATM n'est pas abordée. Pour les raisons ci-dessus, il est clairement nécessaire d'élargir la formation de l'ATSEP dans un contexte de cybersécurité afin qu'ils acquièrent les compétences nécessaires pour aborder tactiquement et stratégiquement les cyberévénements.

1.5 Comme on le sait en Europe, la sécurité n'exige pas seulement que les fournisseurs d'ATS disposent d'un système de gestion de la sécurité, comme c'est le cas pour la sécurité, mais le NPA 2019/07 exige un SMSI (système intégré de gestion de la sécurité) pour tous les ATM/ANS et services habilitants, il existe de nombreuses interfaces supplémentaires, ce qui est également correct, car il s'agit de différentes prestations de services et activités. Cependant, l'incursion et le traitement de la cybersécurité dans la

formation de l'ATSEP à l'échelle mondiale au sein des fournisseurs de services de navigation aérienne (ANSP) sont, au mieux, incohérents et au pire ad hoc.

1.6 Pour comprendre l'impact d'une cyberattaque sur les différentes parties du réseau ATM, il ne suffit pas d'avoir une très bonne connaissance de la technologie informatique et des réseaux IP. Étant donné que les différents réseaux ne sont pas seulement des connexions physiques, mais des informations, des contrôles et des signaux déclenchés par différents facteurs et utilisant différents chemins de transmission tels que la radio, la VoIP, les réseaux, les commandes humaines, les signes lumineux et les signaux, les sons, etc., une compréhension approfondie des mesures d'atténuation de la cybersécurité et de leur impact sur la sécurité du système de gestion du trafic aérien ATM est également requise. Il est également nécessaire d'avoir une formation aéronautique.

1.7 Par conséquent, il est proposé de recentrer et d'élargir le contexte de formation de l'ATSEP dans le Doc 10057, dans Cybersécurité au sein des services ATM/ANS, qui possède une formation aéronautique et une culture de sécurité suffisantes ainsi que les connaissances nécessaires en technologie des réseaux et en informatique, pour faire face aux menaces à la cybersécurité de manière tactique et stratégique.

2. DISCUSSION

2.1 Les objectifs de formation existants contenus dans le Manuel de formation de l'ATSEP (Doc 10057 de l'OACI, deuxième édition 2020) concernant la cybersécurité devraient être revus, mis à jour et, si nécessaire, de nouveaux objectifs de formation créés à la fois dans les objectifs de base et les objectifs de qualification, en mettant l'accent sur la couverture des éléments de cybersécurité de l'information elle-même et des systèmes TIC (technologies de l'information et de la communication), sur la base de l'état actuel de la technique et, dans certains cas, dans la lutte contre les attaques combinées avec les vecteurs d'attaque IT et Signal in Space.

2.2 L'IFATSEA est disposée à apporter son aide à l'OACI pour le développement d'une formation en cybersécurité pour l'ATSEP.

— FIN —