Organisation internationale de l'aviation civile

A41-WP/158
EX/72
2/8/22

NOTE DE TRAVAIL

ASSEMBLÉE — 41e SESSION

COMITÉ EXÉCUTIF

Point 14 : Sûreté de l'aviation — Politique

AIDE APPORTÉE AUX ÉTATS EN TERMES DE RENFORCEMENT DES CAPACITÉS ET DE FORMATION À LA CYBERSÉCURITÉ

(Note présentée par le Guyana et appuyée par l'Argentine, la Bolivie, le Brésil, la Colombie, El Salvador, l'Équateur, le Guatemala, le Panama, le Pérou, la République dominicaine, l'Uruguay et le Venezuela)

RÉSUMÉ ANALYTIQUE

La problématique de la cybersécurité, qui concerne de multiples secteurs, intéresse également le domaine de l'aviation civile. Consciente des menaces qui continuent de peser sur la sûreté de l'aviation civile internationale, l'OACI a élaboré, pour y faire face, une stratégie de cybersécurité et un plan d'action pour la cybersécurité. Si utiles ces politiques et orientations soient-elles pour les États, ces derniers n'en ont pas moins impérativement besoin de connaissances, de compétences, de formations et de ressources afin de pouvoir parer efficacement aux cybermenaces et cyberrisques, et ce tant sur le plan national qu'à l'échelon régional et international.

Aussi, la présente note de travail demande-t-elle à l'OACI de s'investir dans le renforcement des capacités des États afin de leur permettre de réaliser les objectifs des sept piliers de la stratégie, intitulés comme suit :

a) Coopération internationale
b) Gouvernance
c) Législation et réglementation efficaces
d) Politique de cybersécurité
e) Partage d'information
f) Gestion des incidents et planification d'urgence
g) Renforcement des capacités, formation et culture de la cybersécurité.

Suite à donner : L'Assemblée est invitée à :

a) charger le Conseil de demander au Secrétariat de consacrer des ressources à la résilience et au renforcement des capacités des petits États en matière de cybersécurité. Il conviendrait de s'investir, entre autres, dans la sensibilisation au problème de la cybersécurité, dans la formation à la gestion des incidents de cybersécurité et au déploiement de mesures d'intervention en cas d'urgence, dans la formation d'instructeurs spécialisés dans la cybersécurité et dans l'établissement d'un programme de formation qualifiante ;
b) demander à l'OACI de promouvoir et mettre en place un mécanisme de coopération entre les États afin de favoriser les programmes de mentorat et d'échanges techniques dans le domaine de l'aviation.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique *Sûreté et facilitation*.

Références :	Annexe 17 – *Sûreté de l'aviation* *Stratégie de cybersécurité de l'aviation* *Plan d'action pour la cybersécurité*

1. INTRODUCTION

1.1 L'intensification de la circulation aérienne dans le domaine de l'aviation civile est appelée à accroître la dépendance de cette dernière à l'égard de la technologie. Or, une plus grande dépendance à l'égard de la technologie génère davantage de menaces et de risques. D'où l'importance de la cybersécurité pour les États et la nécessité de renforcer leur capacité à y faire face. Dans le secteur aéronautique, la cybersécurité joue un rôle capital car elle touche à de multiples aspects tels que la sûreté, la sécurité, la navigation aérienne, les systèmes de technologies de l'information et des communications et les vols d'aviation générale. La stratégie et le plan d'action de l'OACI en matière de cybersécurité donnent aux États les orientations dont ils ont besoin pour poser les fondements d'une solide infrastructure de cybersécurité. Mais cela suppose un renforcement des capacités, la mise en place de formations, la promotion d'une culture de la cybersécurité et une collaboration inter-institutions et interrégionale.

1.2 S'ils veulent se doter d'une solide infrastructure de cybersécurité, les États devront suivre les sept piliers de la stratégie définie par l'OACI en la matière et adhérer au plan d'action pour la cybersécurité, qui établit les bases d'une collaboration entre les États, les parties prenantes du secteur et l'OACI en vue de renforcer la capacité d'identifier, de prévenir et de détecter les cyberattaques visant l'aviation civile, de les contrer et de se remettre de tels incidents ; il leur faudra aussi définir un cadre de coopération. Le plan d'action propose plusieurs mesures et initiatives que les États devraient entreprendre pour réaliser les objectifs des sept piliers, notamment l'instauration d'une coopération internationale entre les États, l'établissement de structures de gouvernance, la constitution d'un cadre législatif et règlementaire national efficace, la formulation de politiques de cybersécurité, le partage d'informations pertinentes entre les États, la mise en place de mécanismes de gestion des incidents et de planification d'urgence, ainsi que le renforcement des capacités, l'organisation de formations et la promotion d'une culture de la cybersécurité afin d'améliorer la résilience face à ce problème qui touche les pays du monde entier.

1.3 Le renforcement des capacités est indispensable à l'établissement d'une infrastructure de cybersécurité (mondiale) solide. C'est de lui que dépendra la réalisation des objectifs des six autres piliers. Il est donc instamment demandé à l'OACI de favoriser et renforcer les capacités dont les États, en particulier les petits États, ont besoin.

2. ANALYSE

2.1 Le Guyana a lancé plusieurs initiatives pour lutter contre les cyberattaques et améliorer sa capacité à y faire face. Ces initiatives, qui s'inscrivent dans le droit fil des objectifs des sept piliers de la stratégie de cybersécurité dans le domaine de l'aviation, sont chapeautées par une entité nationale - la National Data Management Authority (NDMA) - chargée du contrôle et de la protection des données. La NDMA a commencé à élaborer des politiques, normes, lois et réglementations nationales en matière de cybersécurité qui font l'objet de consultations au sein de comités inter-institutions. Il s'agit d'un processus itératif qui nécessite le concours des organismes concernés, en particulier ceux qui possèdent des infrastructures critiques. Compte tenu des contraintes et difficultés rencontrées par les petits États, il est indispensable de leur donner des orientations et de leur prodiguer des formations qui leur indiquent comment faire globalement pour combattre les risques d'atteintes à la cybersécurité. Les informations seront mises en commun entre les institutions, au plan national, et les formations seront sollicitées *via* le comité inter-institutions ; il n'en est pas moins nécessaire de renforcer les capacités au niveau de l'État.

2.2 Le renforcement des capacités implique de dispenser au personnel aéronautique une formation appropriée afin d'améliorer ses connaissances, compétences, aptitudes et capacités en termes de cybersécurité. Il suppose aussi de mettre à disposition les ressources humaines et les moyens financiers nécessaires pour créer une infrastructure de cybersécurité solide. Il exige également de pouvoir compter sur

un personnel qualifié et expérimenté pour élaborer les textes législatifs et réglementaires relatifs à la cybersécurité. Ces capacités peuvent s'acquérir dans le cadre d'ateliers organisés à l'échelon régional, au plan national et au niveau international. Une formation pertinente et appropriée est nécessaire pour renforcer les capacités des États à gérer les incidents de cybersécurité et à planifier les interventions d'urgence. Il s'agit là d'un impératif dans la mesure où, s'il est impossible d'éviter totalement les cyberattaques, le fait de disposer de robustes systèmes de défense permet d'en atténuer les incidences. Les cyberattaques continueront donc de se produire, mais il est primordial que les États soient en mesure d'améliorer leur résilience pour assurer la continuité des activités.

2.3 L'organisation de séances de formation et d'ateliers et la mise en place de programmes d'apprentissage et de mentorat sont autant de mesures qui sont indispensable pour renforcer les capacités des petits États et qui peuvent être déployées, selon le cas, à l'échelon de différents pays ou d'une région.

3. CONCLUSION

3.1 La présente note de travail reconnaît la nécessité pour les États de renforcer leurs capacités et d'accroître leur résilience en matière de cybersécurité.

— FIN —