Organisation de l'aviation civile internationale

AN-Conf/14-WP/124[1]
29/6/24

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

LIGNES DIRECTRICES CONCERNANT LA RÉGLEMENTATION EN MATIÈRE DE CYBERSÉCURITÉ POUR LES SERVICES DE LA CIRCULATION AÉRIENNE (ATS)

[Note présentée par l'Argentine, avec l'appui de 19 États membres de la Commission latino-américaine de l'aviation civile (CLAC)[2]]

RÉSUMÉ ANALYTIQUE

La présente note contient des réflexions sur l'harmonisation des dispositions réglementaires applicables aux services de la circulation aérienne (ATS), dans le but d'inclure des spécifications, des méthodes et des procédures relatives à d'éventuels scénarios d'attaques menées contre les services ATS à l'aide de logiciels malveillants, afin d'assurer un suivi continu des cours de formation initiale et de remise à niveau du personnel.

Suite à donner : La Conférence est invitée à :
a) appuyer les initiatives contenues dans la présente note de travail, tout en demandant d'analyser la pertinence d'intégrer au cadre mondial de l'aviation des règlements et des méthodes relatifs à la cybersécurité pour les services ATS ;
b) encourager les États à intégrer leurs stratégies nationales de cybersécurité aux stratégies de l'OACI en matière d'aviation civile afin de créer une culture de la cybersécurité dans les services ATS, comprenant des politiques, des stratégies et des mécanismes de protection, en élaborant des dispositions réglementaires proposées.

[1] Version espagnole fournie par l'Argentine.
[2] Aruba (Royaume des Pays-Bas), Belize, Chili, Colombie, Costa Rica, Cuba, République dominicaine, Équateur, El Salvador, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, Uruguay et Venezuela (République bolivarienne du).

1. INTRODUCTION

1.1 L'utilisation croissante, dans l'aviation civile, de technologies de pointe interconnectées à l'échelle mondiale a considérablement accru les risques de cybermenaces.

1.2 À sa 41e session, l'Assemblée de l'Organisation de l'aviation civile internationale (OACI) a souligné l'importance de cette question en intégrant la résolution A41-19 – *Cybersécurité dans l'aviation civile* au document intitulé *Résolutions de l'Assemblée en vigueur (au 7 octobre 2022)* (Doc 10184), Partie VII — *Intervention illicite* ; section *Autres questions relatives à l'intervention illicite*. La résolution invite les États à prendre un certain nombre de mesures ; dont certaines pourraient être appliquées au moyen d'outils réglementaires, ce qui répondrait ainsi aux préoccupations actuelles de la communauté aéronautique quant à l'efficacité des normes, des procédures et des processus existants dans le maintien d'un niveau de risque acceptable dans un environnement numérique connecté.

1.3 Selon un article publié en 2019 par le groupe ALLIANZ intitulé « Baromètre des risques : les principaux risques pour les entreprises » [cité dans la septième édition du *Plan mondial de navigation aérienne* (GANP, Doc 9750)], les formes d'interruption d'activités les plus redoutées sont les cyberattaques par logiciel rançonneur[3]. *WannaCry* et *Petya* sont deux exemples de logiciels rançonneurs utilisés pour attaquer les systèmes numériques dans l'Union européenne. Toutefois, l'article relève que 12 % des cyberinterruptions d'activités sont le fruit de cyberattaques criminelles, tandis que 88 % d'entre elles sont imputables à des pannes techniques ou à des erreurs causées par des interactions humaines avec les systèmes.

1.4 Toutes les parties prenantes de l'aviation civile ont déployé de grands efforts collaboratifs pour protéger et préserver le système de navigation aérienne contre des actes d'intervention illicite, en accordant la priorité à la gestion des risques et à la cyberrésilience des systèmes. Dans ce contexte, les organismes de réglementation de l'aviation civile jouent un rôle fondamental, qui devrait évoluer constamment. Autrement dit, outre les réglementations actuellement en vigueur, il serait utile de proposer des innovations souples et modulables, surtout au regard des nouveaux modèles d'activité en phase de développement, qui devraient privilégier les activités d'entreprise-à-entreprise et/ou d'entreprise-à-consommateur[4]. C'est pourquoi les réglementations devraient définir les normes de performance requises dans ce nouveau contexte, plutôt que de conserver leur fonction antérieure, qui consistait à spécifier de manière très détaillée chaque composante technique.

1.5 Par conséquent, les réglementations devraient faciliter et promouvoir l'innovation, répondre aux exigences de performance et appuyer l'évolution du système de navigation aérienne, tout en assurant également le suivi et la supervision. Dans cette optique, le nouveau paradigme réglementaire marque à bien des égards la transition d'un système centralisé conçu pour deux acteurs seulement [l'organisme de réglementation de l'État et le fournisseur de services de navigation aérienne (ANSP)] à un système réglementaire réparti et coordonné qui offre des services adaptés aux besoins d'une infrastructure cyberrésiliente et aux besoins définis par les usagers.

---

[3] *Un logiciel rançonneur est un type de logiciel malveillant qui chiffre les fichiers d'un utilisateur, puis exige le paiement d'une rançon avant de les restaurer*.

[4] *Plan mondial de navigation aérienne (GANP) en ligne. Modèles de gestion émergents, nouveaux et adaptés, OACI : https://www4.icao.int/ganpportal/GanpDocument/FR#/*

2. ANALYSE

2.1 Compte tenu de ce qui précède, nous présentons un certain nombre de considérations qui favorisent l'alignement et l'harmonisation des dispositions réglementaires applicables aux services ATS. Notre objectif est d'analyser la proposition concernant l'inclusion de spécifications et de procédures pertinentes relatives à d'éventuels scénarios d'attaque utilisant des logiciels malveillants contre les systèmes d'information, tout en répondant aux besoins de toutes les parties prenantes concernées et en assurant un suivi continu de la formation initiale et de remise à niveau afin de veiller à ce que le personnel conserve les compétences requises.

2.1.1 Le scénario d'une cyberattaque contre l'aviation civile est considéré comme une intervention illicite, conformément à la résolution A41-19 – *Cybersécurité dans l'aviation civile*, et en raison de sa nature criminelle.

2.1.2 Les progrès technologiques et l'interconnexion des systèmes de navigation aérienne visent à assurer la sécurité, mais ils peuvent aussi créer les conditions dans lesquelles des interventions illicites peuvent nuire non seulement à l'aéronef, mais aussi aux dépendances des services ATS.

2.1.3 Les normes et pratiques recommandées de l'Annexe 11 – *Services de la circulation aérienne* et les méthodes énoncées dans les *Procédures pour les services de navigation aérienne — Gestion du trafic aérien* (PANS-ATM, Doc 4444) prennent en considération l'intervention illicite par des actions ou des procédures si un aéronef fait l'objet ou est soupçonné de faire l'objet d'une intervention illicite.

2.1.4 Les documents susmentionnés ne couvrent pas l'éventualité d'une attaque contre les systèmes de dépendance des services ATS. Dès lors, il pourrait être capital d'intégrer des orientations réglementaires ou techniques de l'OACI concernant les dépendances des services ATS touchées par les cyberattaques, afin d'établir des procédures adaptées permettant d'apporter des réponses appropriées à ce type d'évènement. Nous proposons d'étudier le scénario de l'intervention illicite dans les services ATS afin d'élaborer des mesures spécifiques visant à contrer les cyberattaques.

2.1.5 Dans cette optique, et conformément au plan d'action de l'OACI pour la cybersécurité, nous suggérons d'analyser s'il est viable ou non d'intégrer des spécifications et/ou des procédures visant à informer l'autorité compétente désignée par l'État lorsqu'une cyberattaque visant une dépendance des services ATS est suspectée ou confirmée, ce qui permettrait un échange rapide d'informations pertinentes entre toutes les parties prenantes concernées, en particulier les exploitants aériens.

2.1.6 En outre, nous pensons qu'il pourrait être essentiel d'instaurer des mécanismes d'échange d'informations sur la cybersécurité entre les autorités militaires et les services de la circulation aérienne afin de pouvoir partager les informations utiles. Ce type d'approche collaborative aiderait à atténuer le risque de cyberattaques à l'encontre des services ATS.

2.2 En outre, et partant du fait que le plan d'action pour la cybersécurité indique la nécessité de « poursuivre l'harmonisation réglementaire aux niveaux mondial, régional et national afin de promouvoir la cohérence à l'échelon au niveau mondial et d'assurer l'interopérabilité des mesures de protection »[5], nous remarquons qu'il faut inclure des dispositions réglementaires spécifiques, sans préjudice de l'adoption d'autres dispositions relatives à cette question, notamment les suivantes :

[5] *Plan d'action pour la cybersécurité, chapitre 3, Plan d'action stratégique, Premier pilier — La coopération internationale, OACI, édition 2022.*

a) des procédures qui couvrent les scénarios de cybermenaces et de cyberattaques au niveau régional, car cela permettrait de surmonter les différences économiques et technologiques que certains États gèrent seuls, d'autant que les cyberattaques ou les cybermenaces se répercutent généralement au-delà des frontières nationales ;

b) des instruments appropriés pour assurer un lien entre la stratégie de cybersécurité des États et les lignes directrices de l'OACI énoncées dans la Stratégie de cybersécurité de l'aviation, garantissant ainsi que l'aviation civile nationale prévoit une politique, une stratégie, une formation et les coûts associés à la mise en œuvre d'une telle stratégie. Il conviendrait également de désigner l'autorité compétente en matière de cybersécurité de l'aviation civile et d'indiquer comment cette autorité communiquera avec les organisations nationales et les autres parties prenantes intéressées ;

c) des dispositions relatives à la sûreté des systèmes de navigation aérienne des États, dont l'architecture garantit l'intégrité et la protection. Il pourrait s'agir de méthodes de signalement, de supervision et d'analyse technique[6] des cyberincidents spécifiques à l'aviation civile ;

d) des dispositions relatives à la formation afin de promouvoir une culture de la cybersécurité au sein des services ATS et de dispenser une formation appropriée à tout le personnel intervenant dans le système de navigation aérienne. Dans ce sens, il serait indispensable de consacrer des projets à la formation de ce personnel ;

e) des mesures d'urgence propres aux services ATS permettant de gérer ces situations et d'assurer la reprise rapide des vols, notamment des mesures de relance en cas de cyberincidents et l'identification des principales parties prenantes pour une communication et une coordination efficaces en cas de crise ;

f) des protocoles de détection et de notification des cyberincidents établissant des procédures claires pour la détection précoce et la notification en temps utile de tout incident de cybersécurité touchant les dépendances des services ATS. Cela garantirait des réponses rapides et coordonnées à toute menace, limitant ainsi les éventuelles répercussions des cyberattaques sur la sécurité et la continuité des vols.

3. CONCLUSION

3.1 La cybersécurité des services ATS est un sujet de préoccupation qui appelle des actions coordonnées aux échelons national, régional et mondial. L'adoption des propositions énoncées dans la présente note constitue un grand pas en avant vers le renforcement de la sûreté du service et l'atténuation des risques associés aux cyberattaques dans les dépendances des services ATS. En adoptant ces approches, les États seraient mieux préparés à faire face aux défis émergents dans le domaine de la cybersécurité, tout en assurant la continuité et l'intégrité des vols. De surcroît, la collaboration internationale et l'harmonisation des réglementations favoriseraient une culture de la cybersécurité forte et résiliente dans la communauté aéronautique mondiale.

[6] L'analyse technique de la cybersécurité est une discipline qui consiste à enquêter sur les incidents relatifs à la sécurité de l'information et à les analyser. Il s'agit notamment des cyberattaques, du vol de données et des intrusions.

3.2 En conséquence, la Conférence est invitée à approuver les mesures suivantes :

a) appuyer les initiatives contenues dans la présente note de travail, tout en demandant d'analyser la pertinence d'intégrer au cadre mondial de l'aviation des règlements et des méthodes relatifs à la cybersécurité pour les services de la circulation aérienne (ATS) ;

b) encourager les États à intégrer leurs stratégies nationales de cybersécurité aux stratégies de l'OACI en matière d'aviation civile afin de créer une culture de la cybersécurité dans les services ATS, comprenant des politiques, des stratégies et des mécanismes de protection, en élaborant des dispositions réglementaires proposées.

— FIN —