Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/243[1]
EX/95
5/8/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

CYBERSÉCURITÉ

[Note présentée par le Conseil international des aéroports (ACI)]

RÉSUMÉ ANALYTIQUE

Les menaces à la cybersécurité sont devenues des risques réels pour le secteur aéronautique et, pour autant qu'on puisse le prévoir, le nombre de ces risques ainsi que leur portée devraient s'accroître. Il est donc essentiel que les parties prenantes de l'aviation mettent sur pied un programme de cyberrésilience et maintiennent des moyens de cyberdéfense solides et efficaces. Toutes les entreprises, dont les aéroports, sont exposées aux cybermenaces, des entreprises qui possèdent un ensemble simple de systèmes à celles qui possèdent des programmes de transformation numérique des plus sophistiqués dans le domaine des TI.

Pour s'attaquer à la cybersécurité, il est manifestement nécessaire de mettre en place une coopération internationale, une gouvernance concertée et des politiques cohérentes et concrètes conjuguées à des moyens concrets pour assurer le partage des informations, la surveillance, le renforcement des capacités et la formation. L'approche cloisonnée actuelle ne permettant pas de traiter cette question efficacement, il est nécessaire que l'OACI développe une vision et une stratégie claires qui tiennent compte de la sécurité, de la sûreté, de l'exploitation et de la résilience, et que l'Organisation travaille conjointement dans tous les domaines.

Suite à donner : L'Assemblée est invitée :

a) à approuver la Stratégie de cybersécurité de l'aviation de l'OACI et à demander que l'OACI travaille avec les États et l'industrie à l'élaboration d'un plan d'action à l'appui de cette stratégie ;
b) à reconnaître la nécessité urgente d'adopter une approche multidisciplinaire en matière de cybersécurité ;
c) à demander que l'OACI réalise sans tarder une évaluation de la structure de gouvernance actuelle dans le domaine de la cybersécurité et à sérieusement envisager la mise sur pied d'un Groupe d'experts chargé de la cybersécurité qui se penchera, de manière globale, sur les questions relatives à la sûreté, à la sécurité, à la résilience et à la continuité de l'exploitation. Le Groupe d'experts doit comprendre des membres compétents et qualifiés provenant des États et de l'industrie pour faire avancer les travaux présentés dans la « Stratégie de cybersécurité » et il devrait être administré conjointement par la Commission de navigation aérienne et, soit le Comité de l'intervention illicite, soit le Comité de transport aérien ;

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

d) à demander que le Conseil fasse participer l'industrie ainsi que les États à l'élaboration de politiques, d'une stratégie, de plans et de normes relatifs à la cybersécurité de l'aviation.	
Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques : Sécurité ; Capacité et efficacité de la navigation aérienne ; Sûreté et Facilitation.
Incidences financières :	Les activités dont il est question dans la présente note de travail seront entreprises sous réserve de la disponibilité des ressources dans le budget du Programme ordinaire de 2020-2022 et/ou de contributions extrabudgétaires.
Références :	A40-WP/28 EX/13, *Stratégie de cybersécurité de l'OACI* Annexe 17, *Sûreté* Doc 8973, *Manuel de sûreté de l'aviation*

1. INTRODUCTION

1.1 Les systèmes aéronautiques sont de plus en plus connectés et l'échange d'informations numériques repose sur l'interdépendance des systèmes des aéroports, des exploitants aériens, des ANSP et des fournisseurs de services d'escale ainsi que des systèmes de transport de passagers.

1.2 Les cybermenaces se sont concrétisées en risques réels pour le secteur de l'aviation et, pour autant qu'on puisse le prévoir, le nombre et la portée de ces risques devraient augmenter. Il est donc d'une importance capitale que les parties prenantes de l'aviation mettent sur pied et maintiennent un programme de cyberrésilience. Toutes les entreprises, dont les aéroports, sont exposées aux cybermenaces, des entreprises qui possèdent un ensemble simple de systèmes à celles qui possèdent des programmes de transformation numérique des plus sophistiqués dans le domaine des TI.

1.3 Qui plus est, il doit être souligné que la question de la cybersécurité ne concerne pas « seulement » la technologie de l'information et des communications (TIC). La cybersécurité est la responsabilité de toute l'Organisation et l'efficacité de la cyberrésilience dépend de l'appui de tous, d'une assurance de la qualité fiable et d'une surveillance étroite, de cadres de politiques bien définis et d'une collaboration efficace entre les parties prenantes. Il est essentiel qu'une culture de sûreté de l'information se développe dans le secteur de l'aviation.

1.4 Les menaces et les incidents liés à la cybersécurité peuvent toucher l'ensemble du système de transport aérien, susciter des préoccupations en matière de sécurité et de sûreté, entraver l'exploitation, entraîner des pertes financières et s'accompagner de répercussions pouvant rapidement dépasser les frontières et toucher le monde entier.

1.5 Une bonne compréhension des cybermenaces sera cruciale pour comprendre et gérer les risques. Il est nécessaire que toutes les parties prenantes de l'industrie aéronautique collaborent afin de promouvoir un dialogue mettant en valeur de multiples points de vue et qu'elles conviennent d'un ensemble commun de mesures.

1.6 Bien que l'industrie aéronautique possède des années d'expérience en matière de sécurité et de sûreté, le défi posé par la cybersécurité est relativement nouveau. L'industrie aéronautique et l'industrie aéroportuaire acquièrent de l'expérience en matière d'atténuation des risques relatifs à la cybersécurité. De ce fait, l'industrie devrait participer à la prise de décisions, sur un pied d'égalité avec

les États, mais aussi à l'élaboration de politiques et de normes dans les organes compétents de l'OACI. Étant donné que la conception et le remplacement de systèmes aéronautiques peuvent prendre davantage de temps qu'il n'en faut à des individus ayant l'intention de mener une attaque pour développer des capacités, il est nécessaire d'adopter une approche qui, d'une part, permet à l'industrie de continuer à mettre en œuvre des meilleures pratiques conformément aux normes internationales existantes comme celles de l'ISO et, d'autre part, favorise une meilleure mise en œuvre à l'échelle mondiale.

1.7 Il est nécessaire d'adopter une approche d'ensemble qui prend en considération la sûreté, la sécurité et la résilience du système de transport aérien, les mesures de protection, les mécanismes d'intervention, le partage des informations, le renforcement des capacités et la surveillance.

2. ANALYSE

2.1 Ces dernières années, l'OACI s'est penchée sur la cybersécurité et la résilience aux attaques contre la cybersécurité au cours de diverses réunions.

2.2 Le Groupe d'experts AVSEC examine actuellement la question de la cybersécurité dans le cadre de la sûreté de l'aviation et il a principalement axé ses travaux sur l'utilisation de la cybersécurité dans l'intention de commettre un acte terroriste visant à nuire à l'aviation. Trois groupes de travail du Groupe d'experts ont étudié cette question en détail.

2.3 Le Groupe de travail sur la menace et les risques (WGTR) a réalisé (en 2015) une analyse des risques d'une attaque délibérée contre la cybersécurité qui pourrait compromettre les systèmes des compagnies aériennes et des aéroports ainsi que les systèmes de navigation aérienne. En ce qui concerne les aéroports, en particulier, les travaux ont principalement porté sur l'altération délibérée de systèmes de sûreté tels que les systèmes de contrôle d'accès et les équipements d'inspection-filtrage de sûreté.

2.4 Le Groupe de travail sur les éléments indicatifs (WGGM) du Groupe d'experts AVSEC a rédigé un chapitre sur la cybersécurité pour le *Manuel de sûreté de l'aviation* (Doc 8973) de l'OACI. Ce chapitre, à un haut niveau, donne un aperçu général aux États, contient des orientations sur l'élaboration d'une évaluation des risques et d'une politique relative aux risques, propose un cadre et traite de l'administration, de la formation, des pratiques en matière de conception, des acquisitions, de la détection, de l'intervention et de la récupération en cas d'incident et du signalement.

2.5 À la suite de longues délibérations sur les SARP tenues par le Groupe de travail sur l'Annexe 17 du Groupe d'experts AVSEC, le Groupe d'experts AVSEC a, dans un premier temps, appuyé deux pratiques recommandées dans l'Amendement n° 15 de l'Annexe 17, lesquelles ont été remplacées par une norme, ainsi qu'une pratique recommandée présentée dans l'Amendement n° 16 de l'Annexe 17, en novembre 2018.

2.6 Afin d'étudier la possibilité d'un réseau de confiance pour la navigation aérienne, le Secrétariat de l'OACI a mis sur pied l'équipe « INNOVA » au sein de la Direction de la navigation aérienne, laquelle est chargée de trouver un moyen de faciliter un échange d'informations sûr, résilient et continu dans un environnement numérique connecté à l'appui des activités actuelles et futures. À cette fin, le Groupe d'étude sur le cadre de confiance (TFSG) a été créé sous l'égide de la Direction de la navigation aérienne pour élaborer un ensemble commun de principes, de politiques et d'orientations ainsi qu'une stratégie de transition à un cadre harmonisé à l'échelle mondiale qui permettra l'échange sol-sol, air-sol et air-air de données et d'informations entre les parties prenantes de l'aviation concernées, au

niveau de résilience et d'interopérabilité nécessaire au maintien d'une capacité et d'une efficacité accrues, dans le but d'assurer la sécurité continue de l'exploitation du système de l'aviation civile.

2.7 L'OACI a mis sur pied le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC), dirigé par le Directeur adjoint de la Sûreté de l'aviation et de la facilitation (DD/ASF). Ce groupe travaille sur des recommandations destinées à l'OACI relatives à la stratégie, à la politique juridique et aux besoins généraux des États et de l'industrie en ce qui concerne la cybersécurité, mais la portée de ses travaux et sa participation sont limitées.

2.8 Le Groupe d'experts des systèmes d'aéronef télépiloté (RPAS) a élaboré des normes relatives à l'échange d'informations entre les aéronefs télépilotés et les postes de télépilotage pour réduire au minimum l'ampleur possible de tout contrôle non autorisé et en atténuer les conséquences.

2.9 Le Comité juridique examine l'efficacité des instruments existants de droit aérien international pour contrer les cybermenaces contre l'aviation civile.

2.10 L'ACI estime que l'OACI est l'Organisation la plus compétente pour prendre des mesures relatives à la cybersécurité aéronautique. Cela étant, la séparation actuelle des activités de cybersécurité à l'OACI décrites plus haut ne permet pas de suivre une approche efficace et globale.

2.11 L'ACI estime qu'il n'est pas nécessaire d'imposer des normes détaillées ou prescriptives relatives à la cybersécurité. En effet, celles-ci pourraient être contreproductives puisqu'il s'agit d'une question changeante qui évolue rapidement et nécessite des interventions flexibles et adaptables. Les approches varient selon les États, les différentes responsabilités étant réparties entre plusieurs organes. Pour ces raisons, la mise en œuvre d'un ensemble de normes visant exclusivement l'aviation serait difficile et complexe.

2.12 Cela dit, la coopération internationale, la gouvernance concertée ainsi que des politiques cohérentes et concrètes sont nécessaires pour s'attaquer à ces questions. Outre la mise en œuvre de moyens concrets pour assurer le partage des informations, la surveillance, le renforcement des capacités et la formation, il est urgent d'élaborer une stratégie et un plan d'action pour l'aviation civile.

2.13 Ce plan d'action devrait promouvoir et faciliter l'élaboration de lignes directrices, de normes et d'outils de mesure communs, la sensibilisation et l'échange de connaissances sur la cybersécurité pour l'écosystème aéronautique. En outre, les initiatives de sensibilisation et l'échange de savoir-faire et de pratiques entre les parties prenantes de l'aviation devraient être appuyés pour tirer parti des leçons apprises et des bonnes pratiques existantes.

3. CONCLUSION

3.1 L'ACI appuie sans réserve la note de travail du Secrétariat de l'OACI concernant la Stratégie de cybersécurité et continuera de jouer un rôle actif dans son élaboration et sa mise en œuvre futures.

3.2 Il est essentiel que l'OACI, les États et l'industrie accélèrent les travaux dans ce domaine, et qu'ils travaillent ensemble dans tous les domaines pour s'attaquer à la cybersécurité. Il ne s'agit pas d'une question pouvant être abordée séparément sur les plans de la sécurité, de la sûreté, de l'exploitation, de la navigation aérienne et de la facilitation vu qu'elle chevauche tous les domaines. L'évaluation des

risques, les éléments indicatifs, l'élaboration de politique et la surveillance s'appliqueront à tous les domaines.

3.3 À condition d'être doté de ressources suffisantes, un Groupe d'experts de la cybersécurité pourrait éventuellement examiner les questions précisées plus haut en offrant :

a) un éventail plus vaste de compétences techniques et d'expérience parmi les membres du Groupe d'experts, en particulier sur le sujet de la cybersécurité ;

b) une approche globale de l'évaluation des risques qui comprend des méthodologies convenues et bien comprises par toutes les parties prenantes et s'appuie sur l'expérience régionale et nationale ;

c) la capacité de créer des groupes de travail afin d'accorder davantage de temps et d'allouer davantage de ressources à l'élaboration d'éléments indicatifs et de programmes, au renforcement des capacités, à l'assistance et à la formation, selon les besoins ;

d) la possibilité d'examiner les questions relatives à la navigation aérienne, à la sécurité et à la sûreté à un seul endroit.

— FIN —