



NOTE DE TRAVAIL

TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 9 – 19 octobre 2018

COMITÉ A

Point 5 : Questions émergentes

5.4 : Cyber-résilience

CYBERRÉSILIENCE

(Note présentée par le Secrétariat)

RÉSUMÉ ANALYTIQUE

Il est important que l'aviation civile soit dotée d'une stratégie appropriée en matière de cyberrésilience. Cette question essentielle a été reconnue au niveau mondial et il faudra l'aborder dans l'édition 2019 du *Plan mondial de navigation aérienne (GANP)* (Doc 9750). Pour gérer efficacement la cyberrésilience dans un système aéronautique de plus en plus interconnecté, il faut se munir d'une stratégie mondiale harmonisée entre toutes les parties prenantes. Sans cadre de confiance coordonné au niveau mondial pour assurer l'échange sécurisé d'informations sol-sol, air-sol et air-air, et sans volonté d'encourager une culture de confiance propice à l'échange de renseignements sur les cyberincidents, la cyberrésilience ne peut être garantie. Il est également reconnu que, malgré la dépendance croissante à l'égard des technologies de l'information, les interventions humaines sont à la fois l'une des causes principales des cybermenaces et le premier rempart contre elles. C'est pourquoi le personnel opérationnel devrait être formé pour reconnaître les aspects généraux des cybermenaces et pour signaler tout soupçon de cybermenace ou de cyberincident.

Suite à donner : La Conférence est invitée à approuver la Recommandation 5.4/x — Cyberrésilience, figurant au paragraphe 3.

Objectifs stratégiques :

La présente note de travail se rapporte aux Objectifs stratégiques Sécurité et Capacité et Efficacité de la navigation aérienne.

Incidences financières :

Incidences pour la communauté aéronautique :

L'introduction de politiques, de technologies et de procédures pour garantir la cyberrésilience peut avoir des incidences financières importantes pour certaines parties prenantes. Celles-ci dépendront toutefois de la taille de l'activité aéronautique et de l'infrastructure d'appui. Il peut y avoir également des incidences sur la sécurité, l'efficacité, les finances et la réputation si la cyberrésilience du système de navigation aérienne ne peut être assurée.

	<i>Incidences pour l'OACI (par rapport aux ressources actuellement prévues au budget du Programme ordinaire) :</i> Étant donné que les activités de planification, d'élaboration et de mise en œuvre au niveau des États d'un cadre de confiance mondial et de renforcement de la sensibilisation à la cyberrésilience se poursuivront pendant les prochains triennats, des ressources supplémentaires, tant financières qu'humaines, sont nécessaires pour soutenir les efforts de l'OACI dans les domaines hautement spécialisés associés à la cyberrésilience et au cadre de confiance.
Références :	Annexe 1 — <i>Licences du personnel</i> Annexe 6 — <i>Exploitation technique des aéronefs</i> Annexe 8 — <i>Navigabilité des aéronefs</i> Annexe 10 — <i>Télécommunications aéronautiques</i> Annexe 11 — <i>Services de la circulation aérienne</i> Annexe 14 — <i>Aérodromes</i> Annexe 15 — <i>Services d'information aéronautique</i> Annexe 17 — <i>Sûreté — Protection de l'aviation civile internationale contre les actes d'intervention illicite</i> Annexe 19 — <i>Gestion de la sécurité</i> Doc 9854, <i>Concept opérationnel d'ATM mondiale</i> Doc 9750, <i>Plan mondial de navigation aérienne</i> Doc 9896, <i>Manuel sur le réseau de télécommunications aéronautiques utilisant les normes et protocoles de la suite de protocoles Internet (IPS)</i> Doc 10022, <i>Résolutions de l'Assemblée en vigueur (au 4 octobre 2013)</i> Doc 10039, <i>Manual on System Wide Information Management (SWIM) Concept [Manuel sur le concept de gestion de l'information à l'échelle du système (SWIM)]</i>

1. INTRODUCTION

1.1 Complexe, le système aéronautique est composé d'un tissu de réseaux et d'appareils, toujours plus connectés et interdépendants aux fins de l'échange de données et d'informations numériques. Les parties prenantes du secteur aéronautique comme les États, les exploitants d'aéronefs et d'aérodromes, et les fournisseurs de services de navigation aérienne (ANSP), entre autres, font désormais reposer leurs opérations quotidiennes sur des technologies de l'information et des communications (TIC) interconnectées et interopérables, et font désormais partie d'un écosystème numérique de l'aviation civile. Cette interdépendance est renforcée par des nouveautés comme la gestion de l'information à l'échelle du système (SWIM), l'introduction de systèmes d'aéronefs télépilotes (RPAS), ainsi que l'émergence de nouveaux acteurs et usagers de l'espace aérien qui ne sont pas encore opérationnels.

1.2 L'évolution vers des systèmes d'information interconnectés et interopérables crée aussi de nouvelles vulnérabilités. Les cyberincidents peuvent affecter l'aviation à bien des niveaux et compromettre les performances du système de navigation aérienne. Ils peuvent compromettre l'échange d'informations entre les parties prenantes, altérer directement la sécurité, la capacité et l'efficacité, et entraîner des répercussions potentiellement graves.

1.3 Dans un environnement aéronautique pleinement interconnecté, la cyberrésilience devient indispensable à la sécurité des opérations. Le système aéronautique doit donc renforcer sa résilience face aux cybermenaces. La cyberrésilience peut être définie comme la capacité à résister à une situation où les performances du système de l'aviation seraient réduites du fait de cybermenaces et de

cyberincidents et s'en remettre, notamment, mais non exclusivement, en cas de perte ou de corruption de données et de perturbations du système, comme la perte de connectivité ou d'interopérabilité.

1.4 La cyberrésilience peut être assurée en combinant différentes normes, procédures et méthodes qui contribuent à atténuer les cybermenaces contre des systèmes essentiels à la sécurité et à l'efficacité de l'aviation.

1.5 L'édition 2019 du *Plan mondial de navigation aérienne* (Doc 9750) soulignera l'importance de doter l'aviation civile d'une stratégie appropriée en matière de cyberrésilience, qui est un élément clé pour réaliser la vision énoncée dans le *Concept opérationnel d'ATM mondiale* (Doc 9854). En conséquence, il est nécessaire de mieux sensibiliser les parties prenantes aux cybermenaces, aux vulnérabilités et aux risques qui pèsent sur le système aéronautique afin de poursuivre l'élaboration d'un ensemble de stratégies mondiales cohérentes pour la cyberrésilience de l'aviation civile.

1.6 Reconnaissant l'urgence et l'importance de protéger les infrastructures essentielles et les systèmes d'information et de communication de l'aviation civile contre les cybermenaces, l'Assemblée de l'OACI a lancé un appel lors de sa 39^e session, pour l'adoption d'une stratégie coordonnée pour acquérir des capacités acceptables et adaptées de cyberrésilience à l'échelle mondiale. Dans cette optique, et afin d'améliorer la sensibilisation de toute la communauté aéronautique à cette question, l'OACI a établi le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC) pour examiner les aspects du système de l'aviation internationale qui sont susceptibles d'être affectés par des cyberincidents.

2. ANALYSE

2.1 Un système cyberrésilient est nécessaire pour garantir l'existence d'un cadre riche en informations alimenté avec des données en temps réel, qui permette une analyse et une modélisation prédictives. Associé à un éventail d'outils de décision et d'appui automatisés, il permettra une évolution des services telle qu'envisagée dans le Doc 9854.

2.2 Interconnectivité et cyberrésilience du système grâce à un cadre de confiance

2.2.1 La gestion efficace de la cyberrésilience requiert une stratégie mondialement harmonisée entre toutes les parties prenantes. Il convient de s'entendre sur les modalités d'interopérabilité des systèmes d'information numérique de façon à créer un cadre riche en informations et commun à toutes les parties prenantes de l'aviation. L'échange sécurisé et résilient d'informations, indispensable pour s'adapter aux besoins de l'activité aéronautique qui évolue sans cesse, peut être assuré à l'aide d'un cadre de confiance, comprenant des normes, procédures, méthodes concertées et des accords pour échanger des données numériques entre les systèmes sol-sol, air-sol et air-air, et réguler un système d'identité.

2.2.2 Il est également nécessaire de renforcer la protection des informations échangées entre les parties prenantes, et entre les systèmes, afin d'accroître la cyberrésilience. À cet égard, l'aviation civile internationale peut s'inspirer de modèles adoptés par d'autres secteurs d'activités, qui s'appuient sur des TIC accessibles et éprouvées, comme le concept des cadres de confiance, les certificats numériques et les réseaux privés virtuels utilisant une infrastructure Internet publique.

2.2.3 Enfin, il faut développer et réviser perpétuellement les systèmes et canaux d'échange de données numériques, qui sont essentiels pour la sécurité, à l'aide d'une stratégie de sécurité dès la conception qui permette de garantir la cyberrésilience par différentes techniques et procédures.

2.2.4 Un cadre de confiance mondial permet d'accroître l'interopérabilité et la connectivité des systèmes numériques et, partant, la cyberrésilience. L'élaboration d'un cadre de confiance mondial pour l'aviation devrait être axée sur la gouvernance, les politiques et les exigences globales de performance technique qui seraient mises en œuvre par les parties prenantes de l'aviation souhaitant échanger des données numériques. Des méthodes fragmentées et non concertées au niveau national ou régional seraient inefficaces et plus coûteuses pour toutes les parties prenantes, et à terme, entraveraient la connectivité et l'interopérabilité des systèmes numériques, et réduiraient la cyberrésilience du système aéronautique.

2.2.5 Un cadre de confiance mondial ne peut être établi que par un organe de normalisation bénéficiant de la confiance d'une majorité suffisante de parties prenantes de l'aviation, et offrant par nature toutes les garanties pour coordonner à l'échelle mondiale les politiques, procédures et méthodes destinées à assurer la sécurité et l'efficacité de l'aviation civile.

2.2.6 Un projet de concept des opérations relatif à un cadre de confiance visant à promouvoir un échange sécurisé d'informations est disponible à l'adresse suivante : <https://www4.icao.int/ganportal/trustframework>. Ce projet préliminaire fournit des renseignements supplémentaires sur un cadre de confiance et sera enrichi à l'avenir.

2.3 **Échange d'informations et sensibilisation à la cybersécurité**

2.3.1 Aucune partie prenante de l'aviation ne peut se protéger seule contre toutes les cybermenaces. L'échange d'informations permettrait à toutes les parties prenantes de l'aviation d'être mieux préparées pour faire face à toute une série de cyberincidents et accroître leurs capacités d'atténuation desdits incidents et de réduction des risques. L'échange d'informations sur le cyberspace qui touchent la sécurité opérationnelle contribuerait à renforcer le climat de confiance entre les parties prenantes de l'aviation, ce qui augmenterait à terme la cyberrésilience du système aéronautique et la sensibilisation de toutes les parties prenantes aux cybermenaces.

2.3.2 Toutes les parties prenantes sont également priées de reconnaître que, malgré la dépendance croissante à l'égard des technologies de l'information, les interventions humaines sont à la fois l'une des principales causes des cybermenaces et le premier rempart contre elles. Le personnel opérationnel, à tous les niveaux, devrait être formé à l'identification des caractéristiques générales des cybermenaces et à la notification de tout soupçon de cybermenace ou de cyberincident, aussi banal soit-il.

3. **CONCLUSION**

3.1 Les systèmes aéronautiques continueront d'être interconnectés à un rythme toujours plus rapide et la numérisation du système de l'aviation se poursuivra. Sans cadre de confiance coordonné à l'échelle mondiale, comprenant des exigences en matière de gouvernance, de politiques et de performance technique globale pour l'interconnectivité et l'interopérabilité des systèmes, on ne peut garantir la cyberrésilience de l'aviation. L'échange d'informations sur les cybermenaces et les cyberincidents, combiné à des formations appropriées du personnel, renforce davantage la cyberrésilience. Pour continuer d'assurer la sécurité et l'efficacité de l'aviation dans un système numérique de plus en plus connecté et interopérable, il faut des stratégies harmonisées de cyberrésilience à plusieurs niveaux, qui profitent directement, aujourd'hui et l'avenir, à toutes les parties prenantes.

3.2 Vu l'importance de la lutte contre les cybermenaces et reconnaissant leurs effets sur la résilience du système aéronautique, la Conférence est invitée à approuver la recommandation ci-après :

Recommandation 5.4/x — Cyberrésilience

Il est recommandé que la Conférence :

- a) demande à l'OACI de travailler avec les États, l'industrie et les organisations internationales pour établir un cadre de confiance mondialement harmonisé pour l'aviation, comprenant des exigences en matière de gouvernance, de politiques, de formation et de performance technique globale, pour permettre la mise en place d'un système aéronautique riche en informations et résilient ;
- b) demande à l'OACI d'œuvrer de concert avec les États, l'industrie et les organisations internationales pour promouvoir le cadre de confiance, expliquer ses avantages et faire mieux connaître son importance pour le renforcement de la cyberrésilience ;
- c) prie instamment les États, l'industrie et les organisations internationales de collaborer avec l'OACI pour mieux faire connaître les cybermenaces et les processus de résilience des systèmes, et de coordonner les activités de formation et d'échange d'informations sur les cyberincidents.

— FIN —