Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A40-WP/283
EX/114
5/8/19

ASSEMBLÉE — 40e SESSION

COMITÉ EXÉCUTIF

Point 12 : Sûreté de l'aviation — Politique

APPROCHE STRATÉGIQUE DE LA CYBERSÉCURITÉ DE L'AVIATION

(Note présentée par la France)

RÉSUMÉ ANALYTIQUE

Compte tenu de l'importance croissante des cybermenaces, de nombreux États ont déjà élaboré une approche intersectorielle stratégique et souveraine. Dans le même temps, des approches spécifiques de cybersécurité de l'aviation sont — ou devraient être — élaborées pour assurer la sécurité, la sûreté et la continuité du transport aérien. Ces deux types d'approche ne devraient pas se nuire, mais au contraire, se compléter mutuellement.

En outre, afin de mettre en œuvre efficacement la stratégie de cybersécurité de l'aviation, il est extrêmement important que les activités pertinentes ne deviennent pas une discipline spéciale qui pourrait finalement entraîner des redondances, des doubles emplois ou des incohérences.

Par exemple, pour assurer cette coordination efficace, la France a créé le Conseil pour la cybersécurité du transport aérien, qui fournit déjà des résultats essentiels pour la protection de l'aviation civile contre les cyberattaques.

La stratégie de l'OACI dans ce domaine devrait être saluée et encouragée dans cet esprit, avec la création d'un organe spécial collaboratif et transversal.

Suite à donner : L'Assemblée est invitée :

a) à recommander à tous les États d'établir une coordination nationale efficace entre leur autorité de l'aviation civile et leurs agences compétentes chargées de la cybersécurité, comprenant des mécanismes de coordination aux niveaux aussi bien stratégique qu'opérationnel avec tous les fournisseurs de services et les parties prenantes du secteur ;
b) à souligner l'importance de l'efficacité du travail intersectoriel et de la coordination entre les entités du Secrétariat de l'OACI chargées de la sûreté et de la sécurité, ainsi que leurs équipes et leurs groupes connexes ;
c) à exhorter le Conseil de l'OACI à définir et à créer au sein de l'Organisation un organe intersectoriel de cybersécurité de l'aviation civile, tel qu'un groupe établi conformément au Doc 9482 (Instructions pour les groupes d'experts), pour consolider et harmoniser toutes les activités et la documentation liées à la cybersécurité, y compris le cadre de confiance.

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 visées dans la présente note seront entreprises sous réserve des ressources prévues au budget-programme ordinaire de 2020-2022 ou provenant de contributions extrabudgétaires.
Références :	Note de travail A40-WP/28 EX/13 : *Stratégie de cybersécurité de l'OACI*

1. CONTEXTE

1.1 Au niveau national, les États membres ont la responsabilité d'assurer la sécurité, la sûreté et la continuité de l'aviation civile, en tenant compte de la cybersécurité, comme cela a déjà été demandé par l'Annexe 17 de l'OACI — *Sûreté*. Toutefois, la protection du transport aérien des cyberattaques fait appel à un très large éventail de sujets ainsi qu'à des ressources de natures différentes. Il est par conséquent extrêmement important de définir le champ d'action des autorités de l'aviation civile et donc le rôle de l'OACI dans ce domaine.

1.2 La cybersécurité n'est pas spécifique à l'aviation et de nombreux États ont déjà élaboré des approches et des réglementations intersectorielles stratégiques souveraines. Ils gèrent très souvent la cybersécurité au niveau interministériel, par le biais soit d'une agence spécialisée, soit d'un organe spécial au sein d'un ministère. Cette approche réglementaire ou « souveraine » aborde l'aviation parmi tous les secteurs d'importance vitale.

1.3 Dans le même temps, en particulier dans le domaine de l'aviation civile internationale, différents États imposent des mesures de protection aux opérateurs aériens (aéroports, compagnies aériennes, ANSP, etc.) et aux constructeurs en essayant de les maintenir interopérables, en équilibre et en harmonie avec les processus généraux de gestion de la sûreté et de la sécurité. Tel est l'objectif de l'« approche de la cybersécurité de l'aviation ».

1.4 À ce niveau, pour donner suite aux questions de cybersécurité et atténuer les menaces et les risques connexes, l'OACI a créé le Groupe d'étude du Secrétariat sur la cybersécurité (SSGC), mis en place le cadre de confiance, et a défini une solide stratégie de cybersécurité pour l'aviation.

2. ANALYSE

2.1 La cybersécurité de l'aviation pourrait amener à examiner tous les aspects des activités de transport aérien, y compris ceux pouvant être liés à l'économie, à la réputation, à l'environnement et à la protection de la vie privée. Plusieurs d'entre eux ne présentent aucune spécificité dans le domaine de l'aviation et sont réglementés par d'autres autorités, selon différents cadres. Il ne faut donc pas créer une autre discipline qui pourrait finalement entraîner des redondances ou des incohérences potentielles, mais se concentrer sur la gestion de la sûreté et de la sécurité, qui est déjà importante et nécessitera d'importantes ressources. Les autres aspects de la cybersécurité dans l'aviation devraient alors être régis par une approche réglementaire nationale ou gérés en interne par le secteur.

2.2 Les approches en matière de cybersécurité de l'aviation doivent être bien articulées au niveau national avec les approches souveraines et assurer une mise en œuvre homogène et cohérente. Les

informations en retour du secteur de l'aviation devraient être utilisées pour modifier les dispositions souveraines de cybersécurité, si nécessaire. Réciproquement, les informations et les données de cybersécurité provenant d'autres secteurs peuvent aider à identifier les menaces potentielles pour l'aviation.

2.3 Enfin, au niveau national, l'approche de la cybersécurité de l'aviation devrait tenir compte de l'ensemble du système d'aviation et permettre de gérer de manière exhaustive tous les cyberrisques inhérents aux activités de l'aviation, sans écarter les petits aérodromes ou exploitants, tout en maintenant les exigences proportionnelles aux risques encourus. Elle pourrait donc être considérée comme le moyen d'atteindre les objectifs de l'approche souveraine dans l'ensemble du secteur de l'aviation nationale.

2.4 Au niveau mondial, l'OACI devrait s'efforcer de créer le cadre nécessaire pour assurer cette articulation appropriée entre l'approche souveraine et celle de l'aviation. Conformément aux priorités définies ci-dessus pour les autorités de l'aviation civile, ce cadre devrait préserver les qualités du système mondial de l'aviation mondiale, notamment la sécurité, la sûreté et l'interopérabilité. Il devrait déboucher sur une approche systémique de la cybersécurité en synergie avec les processus de gestion de la sécurité existant dans le monde.

2.5 L'OACI devrait représenter le secteur de l'aviation dans les instances des Nations Unies examinant les approches souveraines de la cybersécurité pour éviter que la non-coordination des mesures nationales en matière de cybersécurité ne nuit à la performance du système général de l'aviation.

3. UNE EXPÉRIENCE DE COORDINATION : LE CAS DE LA FRANCE

3.1 La France a créé en avril 2018 le Conseil pour la cybersécurité des transports aériens (CCTA). Présidé par le directeur général de l'aviation civile, ce conseil réunit toutes les parties prenantes des secteurs public et privé (agence nationale chargée de la cybersécurité, départements ministériels chargés de la défense et de l'intérieur, fabricants d'aéronefs et d'équipements électroniques, et fournisseurs de services aux aéroports, aux compagnies aériennes, à la navigation) et constitue l'organe compétent pour administrer tous les échanges concernant la cybersécurité dans le domaine de l'aviation civile.

3.2 Dans ce contexte, il est apparu clairement que la cybersécurité de l'aviation devait être considérée de manière globale et intégrée, quelles que soient les frontières classiques entre sûreté et sécurité, pour permettre de tirer parti de toutes les synergies possibles et de résoudre les contradictions éventuelles.

3.3 Les travaux intégrés du CCTA ont également montré qu'il est important de définir précisément un vocabulaire commun et une méthodologie partagée afin d'évaluer les différents scénarios. Ceux-ci sont exprimés sous forme d'objectifs classiques de cybersécurité (disponibilité, intégrité, authenticité et confidentialité) appliqués aux ressources essentielles de l'aviation et évalués sur une échelle à quatre niveaux, compatible avec l'évaluation des risques pour la sécurité.

3.4 La cartographie des flux d'informations irriguant l'ensemble des opérations (aéronefs en maintenance, exploitation des aéroports, opérations en vol, opérations liées aux aéronefs au sol…), est actuellement en cours sur la base d'une analyse des risques. Cette cartographie systémique permettra au CCTA d'identifier les flux d'informations essentiels, les systèmes d'information et les limites des

systèmes d'information pertinents pour chaque scénario. Un résultat important attendu de cet exercice est l'établissement d'une hiérarchie partagée de l'importance des scénarios.

3.5 La prochaine étape consistera à évaluer les mesures d'atténuation et/ou les mesures correctives afin de choisir collectivement le moyen le plus efficace de contrer la menace que représente un scénario particulier.

4. CONCLUSION

4.1 Les stratégies nationales et de l'OACI en matière de cybersécurité de l'aviation devraient viser à améliorer la sécurité et la sûreté du système de l'aviation et à préserver la continuité des services de transport aérien.

4.2 Au niveau national, tous les États devraient coordonner la gestion de la cybersécurité dans le secteur de l'aviation et les cadres réglementaires ainsi que les processus de gestion correspondants avec ceux de la sécurité et de la sûreté. Il faudrait mettre en place une coordination nationale efficace entre leur autorité de l'aviation civile et leurs agences compétentes responsables de la cybersécurité, ainsi que des mécanismes de coordination aux niveaux stratégique et opérationnel avec tous les fournisseurs de services d'aviation et les parties prenantes du secteur.

4.3 Les approches de cybersécurité de l'aviation doivent bien s'articuler aux niveaux mondial, régional et national avec les approches souveraines afin de garantir la pleine interopérabilité des mesures de protection et d'atténuation ainsi que des systèmes de gestion des risques.

4.4 Au niveau international, il semble nécessaire de créer au sein de l'OACI un organe intersectoriel de cybersécurité de l'aviation civile, tel qu'un groupe d'experts créé conformément au Doc 9482 — *Instructions pour les groupes d'experts du Comité du transport aérien et du Comité de l'intervention illicite*. En coordination avec les entités du Secrétariat de l'OACI chargées de la sûreté et de la sécurité, il pourrait œuvrer dans tous les domaines d'intervention de l'OACI pour consolider et harmoniser toutes les activités et la documentation liées à la cybersécurité, y compris le cadre de confiance. Entre-temps, le Groupe d'étude du Secrétariat sur la cybersécurité devrait poursuivre ses travaux sur ce sujet.

— FIN —