Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A39-WP/175
EX/64
9/8/16

ASSEMBLÉE — 39e SESSION

COMITÉ EXÉCUTIF

Point 16 : Sûreté de l'aviation — Politique

CYBERSÛRETÉ EN AVIATION CIVILE : MESURES POSSIBLES À PRENDRE PAR LES ORGANISMES DE RÉGLEMENTATION ET LES PARTIES PRENANTES

(Note présentée par l'Afrique du Sud, l'Arabie saoudite, l'Argentine, la Belgique, les Émirats arabes unis, la Fédération de Russie, la France, le Guyana, l'ex-République yougoslave de Macédoine, la Namibie, Nauru, le Népal, le Nigéria, les Pays-Bas, la République de Moldova, la République démocratique populaire lao, le Royaume-Uni, Sainte-Lucie, le Sénégal, la Sierra Leone, Singapour, la Suisse, et Trinité-et-Tobago)

RÉSUMÉ ANALYTIQUE

Les menaces visant le système de l'aviation civile constituent une préoccupation majeure pour toutes les parties prenantes à l'échelle du globe. Une collaboration entre l'OACI, les autorités de sûreté de l'aviation, l'industrie de l'aviation et les autres acteurs du secteur de l'aviation civile est donc cruciale pour renforcer la sensibilisation aux menaces et établir des politiques, des méthodes et des mesures pratiques et durables, notamment dans les domaines de la formation et du renforcement des capacités, afin de se protéger contre ces attaques et en atténuer les répercussions. Compte tenu de l'interdépendance des différents éléments de l'écosystème mondial de l'aviation civile, une coordination étroite est essentielle pour répondre à ces défis.

Suite à donner : L'Assemblée est invitée :

a) à prendre acte du contenu de la présente note, en particulier des mesures que les organismes de réglementation et les parties intéressées pourraient prendre contre les cybermenaces visant l'aviation civile ;
b) à inviter instamment l'OACI à mettre sur pied un cadre mondial pour la cybersûreté à l'intention des parties prenantes de l'aviation civile ;
c) à désigner, au sein de l'OACI, un organisme chargé de l'élaboration d'un cadre mondial et de la coordination avec d'autres organismes compétents de l'OACI et d'autres parties intéressées.

Objectifs stratégiques :	La présente note de travail se rapporte aux Objectifs stratégiques A — *Sécurité*, B — *Capacité et efficacité de la navigation aérienne* et C — *Sûreté et facilitation.*
Incidences financières :	Aucune incidence financière supplémentaire.

Références :	A39-WP/14, *Stratégie complète de l'OACI pour la sûreté de l'aviation (ICASS)* A39-WP/15, *Établissement d'un plan pour la sûreté de l'aviation dans le monde* A39-WP/16, *Exposé récapitulatif de la politique permanente de l'OACI relative à la sûreté de l'aviation* A39-WP/17, *La cybersécurité dans l'aviation civile* Résolution A38-15 de l'Assemblée, *Exposé récapitulatif de la politique permanente de l'OACI relative à la sûreté de l'aviation* Rapport AVSECP/27 (Couverture jaune) Diffusion restreinte (*en anglais seulement*)

1. INTRODUCTION

1.1 Comme dans d'autres secteurs, les cybermenaces contre le système de l'aviation civile ont été reconnus comme constituant une préoccupation majeure. Les terroristes et les personnes mal intentionnées disposent de multiples façons pour mener des cyberattaques contre les fournisseurs de services d'aviation civile et leur infrastructure. Ils peuvent paralyser les opérations d'aviation civile, notamment en envahissant les systèmes de navigation aérienne et de contrôle, en brouillant les systèmes de radar et de communication et en sabotant les divers systèmes aéroportuaires. Jusqu'ici, ces attaques ont été pour la plupart relativement bénignes et sans conséquences graves ; mais une cyberattaque contre les opérations d'aviation civile pourrait fort bien prendre une tournure catastrophique, avec de nombreuses victimes, l'interruption des services d'aviation civile et/ou des dégâts d'infrastructure critique. Ces menaces sont exacerbées par la dépendance croissante des compagnies aériennes, des aéroports, des fournisseurs de service de navigation aérienne et d'autres acteurs (tels que les services d'escale, de maintenance, de sûreté, d'alimentation en carburant, de fret, etc.) envers les systèmes de technologies de l'information et des communications (TIC) pour leur bon fonctionnement.

2. EFFORTS DÉPLOYÉS CONTRE LES CYBERMENACES

2.1 Ces dernières années, les cybermenaces ont fait l'objet d'une attention plus soutenue de la part des acteurs de l'aviation civile. En 2014, l'OACI, l'Association du transport aérien international (IATA), le Conseil international des aéroports (ACI), la Civil Air Navigation Services Organisation (CANSO) et le Conseil international de coordination des associations d'industries aérospatiales (ICCAIA) ont publié un plan d'action conjoint pour répondre à ces menaces. L'IATA a en outre mis au point une trousse d'outils de cybersûreté pour les compagnies aériennes, tandis que de nombreux aéroports, fournisseurs de services de navigation aérienne et avionneurs ont adopté diverses mesures pour renforcer la sûreté de leurs opérations contre les cybermenaces.

2.2 À l'échelle internationale, les spécialistes de la réglementation de la sûreté de l'aviation civile se sont penchés sur les questions de cybersûreté dans le cadre des travaux du Groupe d'experts de la sûreté de l'aviation (AVSECP). Le Groupe de travail sur la menace et les risques de l'AVSECP a présenté à ce dernier une série d'analyses et de conseils sur les risques de cyberattaques, et une coordination a été entamée entre le groupe AVSECP et les groupes d'experts de la sécurité compétents de l'OACI afin de rationaliser les efforts déployés dans ce domaine horizontal.

2.3 Malgré les mesures prises, de nombreux acteurs ont encore du mal à faire face à ces difficultés. Il serait utile d'accentuer la sensibilisation et de promouvoir le dialogue entre les parties prenantes sur la question des cybermenaces, pour en faciliter la compréhension. Des analyses détaillées de ces menaces permettront aux parties prenantes de détecter les failles de sûreté et de prendre les mesures requises pour les combler. En juillet 2015, Singapour a organisé, en partenariat avec l'OACI et l'IATA et avec le soutien de divers États et acteurs de l'industrie, une conférence sur la cybersûreté qui a réuni de nombreux experts de l'écosystème de l'aviation civile pour se pencher sur les cyberattaques. Parmi les participants figuraient les exploitants d'aéroports, les compagnies aériennes, les fabricants de moteurs d'aéronefs, les services d'escale, les services de sûreté, les fournisseurs de matériel de sûreté, les organisations d'aviation civile internationale et les organismes de réglementation. Les principales questions à l'ordre du jour étaient les suivantes :

a) Les menaces et les risques posés par les cyberattaques au système mondial de l'aviation civile : les analyses périodiques de ces menaces et risques par le WGTR peuvent être utilisées par l'OACI et les parties prenantes pour mettre au point des mesures efficaces de prévention et d'intervention ;

b) Considérations relatives aux mesures de prévention et d'intervention, ainsi qu'aux mesures d'urgence et de rétablissement en cas de cyberattaques contre les opérations d'aviation civile ;

c) Mesures prises par certains acteurs pour répondre aux cybermenaces ;

d) Le secteur de l'aviation civile est particulièrement vulnérable, d'une part parce que les cyberattaques ont plus de chance de porter fruit dans un secteur dont les divers éléments constituants sont interdépendants, et d'autre part, parce que le mécanisme de cyberdéfense dont dispose actuellement le secteur de l'aviation civile ne répond pas de manière adéquate à une menace en évolution constante ;

e) Nécessité d'une approche horizontale couvrant l'ensemble du secteur de l'aviation civile, pour assurer une mise en œuvre coordonnée, proportionnée et effective.

3. MESURES POSSIBLES À PRENDRE PAR LES ORGANISMES DE RÉGLEMENTATION ET LES PARTIES PRENANTES

3.1 Un certain nombre de mesures peuvent être prises par les organismes de réglementation et les parties prenantes, dont les suivantes :

a) Il convient d'attribuer de toute urgence la responsabilité de la question, en commençant à **l'échelle mondiale**, là où il serait le plus utile pour **l'OACI d'établir un cadre dans lequel les parties prenantes de l'aviation civile pourront faire face aux cybermenaces**. Ce cadre, à établir sur la base des meilleures pratiques en vigueur relatives à la sûreté des informations et à élaborer en étroite consultation avec les spécialistes de la sûreté et de la sécurité de l'aviation, pourrait consister en une série de principes, de lignes directrices et d'orientations à l'intention des organismes de réglementation et de l'industrie.

b) **À <u>l'échelle nationale</u>, il importe que les autorités de la sûreté de l'aviation (en coordination avec d'autres autorités responsables de la cybersûreté au niveau national) établissent et assurent une surveillance réglementaire pour répondre aux cybermenaces**. Le mécanisme de surveillance réglementaire devrait couvrir le secteur de l'aviation civile et toutes les parties prenantes de l'écosystème de l'aviation civile d'un point de vue holistique, compte tenu de leur interdépendance.

c) **À l'échelle de <u>l'acteur individuel</u>, chacune des parties prenantes devra établir sa propre série de mesures afin de protéger son exploitation contre les cybermenaces, notamment pour les systèmes liés à la sûreté et à la sécurité de l'aviation.**

d) Les parties prenantes doivent riposter le plus tôt possible aux cybermenaces. Il importe donc que le secteur de l'aviation civile **établisse des mesures aux fins de détection précoce, de coordination et d'intervention rapide**. Le signalement des incidents de cybersûreté aux équipe d'intervention en cas d'urgence informatique (CERT) ou aux centres d'échange et d'analyse d'informations (ISAC) permettrait d'alerter rapidement les autres parties prenantes, et il conviendrait d'encourager l'application d'une telle mesure à l'échelle nationale, avec une coordination internationale dirigée par l'OACI.

e) Comme la cybersûreté est mue à la fois par l'évolution de la menace et par les nouvelles tendances technologiques, il s'agira de **regrouper les personnes, les processus, les technologies et les systèmes pour assurer que chacun de ces éléments dispose de la capacité d'identifier et de déjouer les menaces**.

f) **Le partage d'informations et des meilleures pratiques sur la cybersûreté de l'aviation civile entre institutions est essentiel**. Cela aidera les États et les parties prenantes, conjointement et collectivement, à détecter les tendances, identifier les menaces et élaborer des contre-mesures. Il importe par ailleurs que les organismes de renseignement et autres institutions compétentes poursuivent leurs efforts afin d'acquérir une meilleure compréhension des cybermenaces visant l'aviation civile.

g) Compte tenu de la nature interconnectée des systèmes d'information de l'aviation civile, **une compréhension commune de ces systèmes et données est essentielle, voire critique, pour la sûreté, la sécurité et l'exploitation continue des systèmes de l'aviation civile.** Les organismes de réglementation de l'aviation devraient élaborer ensemble des critères pour déterminer quels systèmes sont jugés critiques (sur le plan mondial, régional et/ou national) afin de guider la mise en œuvre.

h) **Il importe de former le personnel dans tout l'écosystème de l'aviation civile, afin de le sensibiliser aux menaces et aux risques que posent les cyberattaques, pour qu'il puisse réagir rapidement et de manière appropriée**. La détection d'anomalies et le lancement d'alertes précoces face à tout événement suspect ou activité suspecte permettraient de prévenir ou de déjouer une cyberattaque et contribuer à réduire au minimum les interruptions de l'exploitation. Il importe donc d'inclure les problèmes de cybersûreté dans les programmes de formation

à la sûreté de l'aviation, ainsi que de recruter des spécialistes et des vérificateurs de la sûreté de l'aviation qui sont bien au fait des questions de cybersûreté.

i) **Il importe également de renforcer la culture de la sûreté de l'aviation, afin de mettre en valeur une meilleure compréhension des cybermenaces**. Si, aux plus hauts niveaux, la nécessité de faire face à ces menaces est reconnue, donnant lieu à un appui solide de la formation du personnel et à des investissements dans les ressources connexes requises, le secteur de l'aviation civile sera alors en mesure de répondre plus efficacement à ces difficultés.

— FIN —