Organisation de l'aviation civile internationale

LC/40-WP/2-7
12/9/26

NOTE DE TRAVAIL

COMITÉ JURIDIQUE — 40e SESSION

(Montréal, 26 – 30 octobre 2026)

Point 2 : Examen du programme général des travaux du Comité juridique

VULNÉRABILITÉS EN MATIÈRE DE CYBERSÉCURITÉ NON COUVERTES ACTUELLEMENT PAR LE DROIT AÉRIEN

(Note présentée par l'Afrique du Sud)

1. INTRODUCTION

1.1 Compte tenu de l'augmentation du nombre de cyberattaques, des menaces qu'elles font peser sur l'aviation civile ainsi que des complexités en ce qui concerne la gestion, la force exécutoire et l'application des instruments juridiques internationaux actuels, il s'avère crucial pour les États d'accélérer l'examen de ces instruments et de combler les lacunes juridiques qui nuisent à l'efficacité des mesures susceptibles d'être prises pour réprimer et prévenir les infractions liées à la cybersécurité.

1.2 Bien que les cyberattaques soient monnaie courante, elles comportent plusieurs complexités qui rendent difficiles l'identification des auteurs, ainsi que la prévention des cyberattaques, la dissuasion et la mise en œuvre des mesures juridiques nécessaires. La présente note examine ces difficultés, dont la résolution nécessitera une approche multidimensionnelle ainsi qu'un engagement de la part des États à mobiliser les ressources nécessaires.

2. ANALYSE

2.1 Le cadre du droit aérien international est mis à l'épreuve par des menaces pour lesquelles il n'a pas été conçu à l'origine. Le problème n'est pas que le droit aérien international ait perdu sa raison d'être, mais il existe des lacunes certaines en matière d'attribution, de compétence juridictionnelle, d'exécution, de responsabilité, de communication d'informations et de traitement des cyberattaques. Cette situation découle d'une exposition croissante à un environnement où plusieurs types de menaces coexistent comme :

a) les cyberopérations commanditées et les perturbations à motivation politique ;

b) les rançongiciels et les attaques visant les systèmes d'enregistrement de passagers et de bagages, des entreprises de transport aérien et d'assistance en escale utilisés dans les aéroports ;

c) le brouillage et le leurrage du Système mondial de navigation par satellite (GNSS);

d) les drones, les missiles et les systèmes de défense aérienne employés à proximité des routes empruntées par l'aviation civile ;

e) les perturbations touchant les services de navigation aérienne, les communications et les chaînes logistiques du secteur de l'aviation ;

f) les activités de cyberactivistes ou de mandataires, dont les commanditaires peuvent être difficiles à identifier ;

g) les modifications rapides de la disponibilité de l'espace aérien en période de crise.

2.2 L'OACI considère que ces risques sont interdépendants, et ne relèvent pas séparément de la « sécurité », de la « sûreté » et de la « cybersécurité ». Les liens entre ces risques sont clairement exposés dans le document de l'OACI *Considérations relatives aux cyberrisques dans le monde* (Doc 10213).

2.3 Cette préoccupation juridique plus générale se manifeste aussi dans la récente prise de position de l'OACI, présentée dans le rapport sur l'analyse des lacunes menée afin de déterminer la nécessité d'établir des normes et des pratiques recommandées (SARP) relatives à la cybersécurité de l'aviation. L'Organisation a pris acte des travaux effectués par l'Équipe spéciale sur les normes et pratiques recommandées relatives à la cybersécurité et des conclusions de cette dernière sur le fait que la protection juridique existante ne suffit pas à elle seule à protéger les aéronefs civils en cas de crise liée à une cyberattaque. Ce constat souligne combien il est urgent de pouvoir communiquer des informations rapidement, de procéder à des évaluations des risques plus rigoureuses et d'assurer la coordination entre les différents intervenants aux niveaux national et international lorsqu'une cyberattaque se produit.

2.4 **Lacunes recensées**

2.4.1 Les instruments juridiques internationaux ne permettent pas toujours de clairement qualifier les cyberattaques d'actes d'intervention illicite. Les questions que soulèvent souvent les cyberattaques qui compromettent la sécurité et la sûreté de l'aviation civile sont les suivantes :

a) À partir de quel moment une perturbation des systèmes de navigation aérienne ou des systèmes aéroportuaires constitue-t-elle une attaque contre l'aviation civile plutôt qu'un simple cybercrime ?

b) À partir de quel niveau de perturbation peut-on considérer qu'il existe une menace pour la sécurité et la sûreté de l'aviation ?

c) Comment faut-il qualifier une cyberattaque qui entraîne des perturbations économiques, mais n'occasionne ni dommages matériels ni accidents d'aviation ?

2.5 Le cadre juridique international actuel repose sur attaques classiques contre des biens matériels, telles que le détournement ou la destruction d'aéronefs, ou les attaques contre des installations de l'aviation, plutôt que sur des cyberattaques susceptibles, au départ, de compromettre l'intégrité des données ou les processus de traitement des passagers.

2.6 **L’attribution reste le principal point faible**

2.6.1 Bien que les enquêteurs puissent identifier l’infrastructure, la famille de logiciels malveillants ou le modus operandi employés pour une attaque, il est en revanche plus complexe et plus difficile d’établir avec certitude l’identité de l’auteur de l’attaque. Il en résulte un vide en matière de responsabilité, lorsque :

a) l’opération a été menée par un groupe de mandataires ;

b) l’infrastructure est répartie entre plusieurs pays ;

c) le groupe utilise des systèmes compromis appartenant à des tiers innocents ;

d) un État apporte son soutien, mais ne dirige pas ouvertement l’opération ;

e) l’État dont relève la victime ne peut pas divulguer les renseignements qui étayent sa conclusion ;

f) l’attaquant nie toute implication et tout intérêt dans cette affaire.

2.7 Les cyberattaques sont sophistiquées et ne correspondent pas aux modes conventionnels d’attaque de sécurité ou de sûreté.

2.8 **La compétence juridictionnelle est fragmentée**

2.8.1 Un seul cyberincident dans le secteur de l’aviation peut impliquer :

a) un aéroport ou une entreprise de transport aérien situés dans différents États concernés ;

b) un fournisseur de services infonuagiques situé dans un autre pays ;

c) un fournisseur de logiciels ou de matériel situé dans un autre pays ;

d) une infrastructure d’attaque répartie sur plusieurs territoires ;

e) des passagers de nombreuses nationalités ;

f) un attaquant ou un groupe mandataire opérant à partir d’un État qui refuse de coopérer.

2.9 **Responsabilité et indemnisation**

2.9.1 La *Convention pour l’unification de certaines règles relatives au transport aérien international* (Montréal, 1999) établit des règles importantes en matière de responsabilité des entreprises de transport aérien, mais elle n’a pas été conçue comme un instrument exhaustif de répartition des risques liés aux cybermenaces. D’une cyberattaque peuvent découler des questions épineuses, notamment :

a) Qui assume les pertes subies par les passagers à la suite d’une cyberattaque contre un aéroport ?

b) L’annulation d’un vol causée par un rançongiciel constitue-t-elle une circonstance extraordinaire ?

c) Dans quels cas une entreprise de transport aérien peut-elle être tenue responsable d'un manquement à son obligation d'assurer sa cyberrésilience ?

d) Quelles responsabilités incombent à un exploitant d'aéroport, à un fournisseur de services de navigation aérienne, à un fournisseur de services infonuagiques ou à un fournisseur d'équipements ?

e) Comment répartir la responsabilité lorsque plusieurs organisations ont contribué à une vulnérabilité ?

f) Une cyberattaque visant les systèmes d'enregistrement des bagages ou des passagers entraîne-t-elle les mêmes conséquences juridiques qu'une attaque visant les systèmes de sécurité d'un aéronef ?

2.10 L'absence d'un cadre juridique international harmonisé régissant les questions relatives à la responsabilité des acteurs d'une chaîne logistique et aux perturbations des activités découlant de cyberattaques peut donner lieu à une attribution non uniforme des responsabilités entre les différentes compétences.

3. CONCLUSION

3.1 Les instruments internationaux actuels de l'aviation civile ne prévoient pas de système centralisé et complet de compétence, d'enquête, de poursuite et d'indemnisation des victimes dans le cas de cyberincidents transfrontaliers touchant l'aviation. Dans la pratique, la responsabilité peut être répartie entre le droit pénal national, la réglementation aérienne, le droit relatif à la protection des données, le droit des télécommunications, le droit des contrats et le droit international.

3.2 Il est nécessaire que l'OACI prenne des mesures pour mobiliser, par l'intermédiaire des États, les ressources requises pour élaborer un cadre juridique complet qui tient compte des cyberincidents sous toutes leurs formes et de toutes les difficultés qui y sont associées.

4. SUITE À DONNER PAR LE COMITÉ

4.1 Le Comité juridique est invité à :

a) prendre acte des travaux en cours pour analyser la mesure dans laquelle les instruments juridiques internationaux existants permettent de résoudre les difficultés associées aux cyberincidents qui compromettent la sécurité et la sûreté de l'aviation civile ;

b) poursuivre les travaux visant à définir un cadre juridique international qui couvre non seulement les menaces conventionnelles de sécurité et de sûreté mais qui tient compte des risques moins visibles et de plus en plus complexes liés aux cyberattaques.

— FIN —