Organización de Aviación Civil Internacional

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

NOTA DE ESTUDIO

COMITÉ JURÍDICO – 40º PERÍODO DE SESIONES

(Montreal, 26 – 30 de octubre de 2026)

Cuestión 2: Consideración del programa general de trabajo del Comité Jurídico

VULNERABILIDADES DE CIBERSEGURIDAD NO CONTEMPLADAS EN EL DERECHO AERONÁUTICO VIGENTE

(Nota presentada por Sudáfrica)

1. INTRODUCCIÓN

1.1 Teniendo en cuenta el aumento de los ataques de ciberseguridad, las amenazas que suponen para la aviación civil y las complejidades en la gestión, aplicabilidad y ejecución de los instrumentos jurídicos internacionales en vigor, es fundamental que los Estados agilicen el examen de dichos instrumentos y zanjen los vacíos legales que dificultan la eficacia de las medidas que pueden adoptarse para perseguir y disuadir los delitos relacionados con la ciberseguridad.

1.2 Aunque los ataques de ciberseguridad son frecuentes, hay numerosos aspectos complejos que dificultan la detección, disuasión y prevención de sus responsables y la aplicación de las medidas jurídicas necesarias. Esta nota examina aquellas complejidades que requerirán distintos enfoques inmediatos y el compromiso de los Estados para aportar recursos que las resuelvan.

2. ANÁLISIS

2.1 El marco del derecho aeronáutico internacional se está poniendo a prueba con la gestión de amenazas para las que no fue diseñado originalmente. La cuestión no es que el derecho aeronáutico internacional sea ahora irrelevante, sino que hay una serie de lagunas claras en la atribución, jurisdicción, aplicación, responsabilidad, intercambio de información y tratamiento de los ataques de ciberseguridad, ya que aumenta la exposición a un entorno de amenazas múltiples que implica lo siguiente:

a) respaldo a operaciones cibernéticas y disrupciones motivadas políticamente;
b) programas secuestradores y ataques contra los sistemas de facturación y manipulación de equipajes en aeropuertos, de las aerolíneas y de los servicios de escala;
c) interferencia y suplantación de señales en el sistema mundial de navegación por satélite (GNSS);
d) drones, misiles y sistemas de defensa aérea próximos a rutas aéreas civiles;
e) interrupción de los servicios de navegación aérea, de las comunicaciones y las cadenas de suministro de aviación;
f) pirateo informático y acciones por encargo cuya responsabilidad no es fácil de atribuir; y
g) cambios rápidos en la disponibilidad del espacio aéreo en tiempos de crisis.

2.2 La OACI trata estos riesgos como interconectados en lugar de como asuntos separados de "seguridad operacional", "seguridad de la aviación" y "ciberseguridad". Los nexos de este riesgo están bien articulados en las *Consideraciones sobre ciberriesgos mundiales* (Doc 10213) de la OACI.

2.3 La preocupación jurídica general también se plasma en el reciente reconocimiento de la OACI, según consta en el informe *Gap Analysis on the Need for Aviation Cybersecurity SARPs* [Análisis de carencias sobre la necesidad de SARPS de ciberseguridad de la aviación], al reconocer el trabajo y las conclusiones del Equipo Especial sobre Normas y Métodos Recomendados de Ciberseguridad, que señalan que la protección jurídica actual no basta por sí sola para proteger aeronaves civiles en caso de crisis causada por ciberataques, a lo que se suma la necesidad acuciante de proceder a un intercambio rápido de información, una evaluación de riesgos más sólida y una coordinación entre entidades varias a nivel nacional e internacional en caso de ciberataque.

2.4 **Carencias detectadas**

2.4.1 Los ciberataques no siempre se clasifican debidamente en virtud de los instrumentos jurídicos internacionales como actos de interferencia ilícita. Aquellos que afectan a la seguridad operacional y la protección de la aviación civil suelen plantear las siguientes preguntas:

a) ¿Cuándo supone una disrupción de los sistemas de navegación aérea o aeroportuarios un ataque a la aviación civil en lugar de un ciberdelito ordinario?
b) ¿Qué grado de interrupción constituye una amenaza para la seguridad y protección de la aviación?
c) ¿Cómo debería tratarse un ciberataque cuando causa una interrupción económica pero no hay daños físicos ni accidentes aéreos?

2.5 El marco jurídico internacional en vigor se define en torno a actos físicos tradicionales como el secuestro, la destrucción de aeronaves o ataques contra instalaciones de aviación y no tanto en relación con ciberataques que pueden afectar en un principio a la integridad de los datos o la gestión del público pasajero.

2.6 **La atribución sigue siendo la principal debilidad**

2.6.1 Aunque en la investigación sea posible identificar la infraestructura, el tipo de programa malicioso o el patrón operativo de un ataque, demostrar quién es responsable del ataque es más complejo y difícil, lo que en la práctica genera un vacío en la rendición de cuentas:

a) un grupo realiza la operación por encargo;
b) la infraestructura se encuentra en varios países;
c) el grupo utiliza sistemas comprometidos pertenecientes a terceros inocentes;
d) un Estado proporciona apoyo pero no dirige abiertamente una operación específica;
e) el Estado de la víctima no puede divulgar públicamente información que permita su conclusión; y
f) la parte atacante niega su implicación y beneficios.

2.7 Los ciberataques son sofisticados y no se ajustan a las formas convencionales de seguridad y protección contra ataques.

2.8 **La jurisdicción está fragmentada**

2.8.1 Un solo incidente cibernético en la aviación puede implicar lo siguiente:

a) aeropuerto o aerolínea afectados en varios países;
b) proveedor en la nube ubicado en otro país;
c) proveedor de soporte lógico o equipos de otro país;
d) infraestructura de ataque en varias jurisdicciones;
e) público pasajero de múltiples nacionalidades; y
f) atacante o grupo por encargo que opera desde un Estado que no está dispuesto a cooperar.

2.9 **Responsabilidad e indemnización**

2.9.1 Aunque el *Convenio para la Unificación de Ciertas Reglas para el Transporte Aéreo Internacional* (Montreal, 1999) establece normas importantes de responsabilidad de las aerolíneas, no fue diseñado como instrumento integral de atribución de riesgos cibernéticos. Hay preguntas difíciles que surgen tras un ciberataque, por ejemplo:

a) ¿Quién abona las pérdidas sufridas por el público pasajero en caso de ciberataque a un aeropuerto?
b) ¿La cancelación de vuelos causada por programas secuestradores se considera una circunstancia extraordinaria?
c) ¿Cuándo es responsable una aerolínea por no mantener la ciberresiliencia?
d) ¿Qué responsabilidad asume un aeropuerto, proveedor de servicios de navegación aérea, proveedor en la nube o proveedor de equipos?
e) ¿Cómo debería asignarse la responsabilidad cuando son varias las organizaciones que contribuyeron a la vulnerabilidad?
f) ¿Un ciberataque que afecta a los sistemas de equipaje o facturación genera las mismas consecuencias legales que un ataque que afecta a los sistemas de seguridad operacional de las aeronaves?

2.10 La ausencia de un marco jurídico internacional armonizado que contemple cuestiones relacionadas con la responsabilidad en la cadena de suministro y la interrupción operacional por motivos cibernéticos puede derivar en resultados incoherentes entre jurisdicciones.

3. CONCLUSIÓN

3.1 Los instrumentos vigentes de aviación civil internacional no crean un sistema jurisdiccional completo y centralizado para la investigación, el enjuiciamiento y la compensación de las víctimas por incidentes cibernéticos transfronterizos en aviación. En la práctica, la responsabilidad puede abordarse desde el derecho penal nacional, la reglamentación de la aviación, la protección de datos, las normas de telecomunicaciones, el derecho contractual y el derecho internacional.

3.2 Es necesario que la OACI tome medidas para movilizar recursos a través de los Estados con el fin de elaborar un marco jurídico integral que recoja todas las combinaciones y desafíos que plantean los incidentes de ciberseguridad.

4. MEDIDA PROPUESTA AL COMITÉ

4.1 Se invita al Comité Jurídico a:

a) reconocer el trabajo actual de análisis de la aplicabilidad de los instrumentos jurídicos internacionales vigentes para abordar los desafíos que plantean los incidentes de ciberseguridad que afectan a la seguridad y protección de la aviación civil; y

b) continuar con la labor para valorar un marco jurídico internacional que contemple no solo las amenazas tradicionales de seguridad y protección, sino que también cubra los riesgos menos visibles y cada vez más complejos que generan los ciberataques.

— FIN —