

UNDÉCIMA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, 22 de septiembre - 3 de octubre de 2003

Cuestión 2 del

orden del día: Seguridad y protección en la gestión del tránsito aéreo (ATM)

2.5: Seguridad y protección de la infraestructura ATM

SEGURIDAD EN LAS COMUNICACIONES ATM

(Nota presentada por Italia)

RESUMEN

El transporte aéreo se debe considerar como "Infraestructura nacional crítica (CNI)", y por lo tanto las comunicaciones ATM, que incluyen las subredes móviles y fijas, se deben considerar como infraestructuras de información críticas (CII). En esta nota se presentan algunos aspectos específicos de los sistemas CNI-CII importantes para la seguridad, tales como el cifrado, la conectividad, la calidad del servicio y otros.

Italia propone utilizar las iniciativas estratégicas de EUROCONTROL y definir orientaciones para el mejoramiento de la seguridad de las comunicaciones de la gestión del tránsito aéreo.

Las medidas propuestas a la Conferencia figuran en el párrafo 4.

1. INTRODUCCIÓN

1.1 Actualmente los Estados y organizaciones supranacionales se basan, para su crecimiento y organización interna, en sistemas de infraestructura cada vez más complejos y amplios como, por ejemplo, la distribución de la energía eléctrica, el transporte, las comunicaciones públicas, etc. Esto requiere una correlación sólida entre la seguridad y la vulnerabilidad de dichas estructuras y la eficacia del sistema en su conjunto.

1.2 Además, después del ataque del 11 de septiembre, las organizaciones que desempeñan un papel crítico dentro de los contextos nacionales e internacionales tienen que volver a examinar su enfoque con respecto a la seguridad y la supervivencia de las infraestructuras.

1.3 Esa infraestructura crítica se ha definido como infraestructura nacional crítica (CNI), y la “defensa” esencial se ha convertido en una prioridad urgente.

1.4 El transporte aéreo debe considerarse un componente importante del CNI y, en el marco de la gestión del tránsito aéreo (ATM), las redes de telecomunicaciones e información correspondientes, fijas y móviles, se tienen que considerar un CNI, más exactamente, una infraestructura de información crítica (CII).

1.5 En el marco descrito, Italia propone la utilización de las iniciativas estratégicas de EUROCONTROL y la elaboración de un conjunto coordinado de medidas que se centre en la manera en que puede mejorarse la seguridad de las comunicaciones de la gestión del tránsito aéreo.

2. CII FIJAS Y MÓVILES

2.1 Comunicaciones fijas

2.1.1 Las principales características esenciales para garantizar una CII segura son las siguientes:

- a) **Redundancia de la topología:** La CII se debe planificar para que tenga una gran conexión con los nodos centrales (se aconseja un grado mínimo de 3) y con los nodos de acceso y centrales (se recomienda “doble recalada”);
- b) **Portadores de transmisión de alta calidad:** Un CII debería garantizar un flujo de información correcto y oportuno en todas las circunstancias, tanto de manera regular como en emergencias. Se debe proporcionar a los usuarios la anchura de banda necesaria y el servicio de calidad (QoS) acordado. Por lo tanto, se deben utilizar conexiones de alta capacidad y núcleos de conmutación inteligentes. Para cumplir con los requisitos de redundancia los enlaces deben ser de diferentes tipos, entre los que se incluyen enlaces de radio de alta capacidad [línea de lado (LoS)] y satélite (SAT), y cables de fibra óptica (FOC). Para garantizar una gestión eficaz de la anchura de banda, los enlaces deben pertenecer al mismo CII y posiblemente estar separados de las líneas públicas;
- c) **Inteligencia de red distribuida:** La CII deberá ser capaz de proporcionar servicios vocales y de datos con la calidad necesaria. Debería optimizar dinámicamente la distribución de recursos de la red general, encontrar las trayectorias menos congestionadas y posiblemente explotar la redundancia en tipos de conexión y en tipología de red. Además, la CII debería tratar flujos de tráfico con diferentes prioridades, en conformidad con las diferentes clases de servicios, y debe ser capaz de reconocer las conexiones con menor prioridad en caso de emergencia o si se dispone de una anchura de banda reducida. La tecnología de modo de transferencia asíncrono, que originalmente incorpora casi todas estas características, se considera la mejor posibilidad disponible para la infraestructura de transmisión latente y planes de control de gestión de la red;
- d) **Características de seguridad:** La CII además de una defensa contra intrusiones “físicas” también transporta datos críticos CNI que se deben asegurar contra partes no autorizadas o su modificación. Este tema se debe tratar por medio de cifrado y cortafuegos. Los cortafuegos se deben aplicar en las fronteras de los dominios nacionales y deberían estar configurados de manera adecuada. Esto es especialmente importante en el caso de accesos a distancia en estaciones de control y podría incluir mecanismos de autenticación sólidos, ajustados de manera adecuada para los

diferentes niveles de acceso (de acuerdo con el principio “necesidad de saber” originado militarmente). Además, se recomienda firmemente que el tráfico crítico (como las contraseñas o claves de autenticación, y la información sobre controles o sistemas) podría circular en la red en forma cifrada para evitar la detección externa de topología CNI y ubicaciones de recursos críticos internos por medio del análisis de tráfico; y

- e) **Interoperabilidad eficaz y capacidades de integración:** La CII debería diseñarse para que sea interoperable, hasta donde sea posible, con normas de intercomunicación y debe estar integrada con sistemas de desprendimiento fijos y móviles.

2.2 Comunicaciones móviles

2.2.1 Las características principales que se necesitan para un componente aire-tierra CII seguro son las siguientes:

- a) **Evitar la intrusión no autorizada:** las comunicaciones aire a tierra se pueden ver fácilmente utilizando un receptor comercial que se vende al público. Esta cuestión se debe tratar con cifrado y autenticación de la fuente de la información o por medio de otras soluciones apropiadas;
- b) **Capacidad para funcionar ante interferencias (interferencias deliberadas):** se puede interferir de manera deliberada fácilmente las comunicaciones aire-tierra utilizando un transmisor comercial. Esto se debe tratar por medio de saltos de frecuencia o transmisiones con ensanchamiento del espectro u otras soluciones apropiadas;
- c) **Capacidad para funcionar en presencia de interferencia (interferencia por simulación de señales):** las comunicaciones aire a tierra se pueden engañar fácilmente (o interferir por simulación de señales) utilizando un transmisor comercial. Esta cuestión se puede tratar por medio de autenticación de mensajes; también puede ser útil los saltos de frecuencia o el ensanchamiento del espectro;
- d) **Integridad de los datos:** la existencia de un enlace alternativo en la comunicación aire-tierra (por ejemplo un enlace de comunicación por satélite) debería ser el medio de garantizar el nivel de alta integridad de los CII móviles con referencia de la información crítica y sensible; y
- e) **Separación física:** para garantizar la gestión de comunicaciones efectiva las comunicaciones aire-tierra ATM deberían separarse en lo posible de otros servicios de aire-tierra como Internet, correo electrónico, comunicaciones públicas, cable de televisión y comunicaciones a la aeronave de la compañía [sistema de direccionamiento e informe (ACARS) y control de las operaciones aeronáuticas (AOC)].

3. INICIATIVA ESTRATÉGICA PROPUESTA

3.1 Se propone elaborar y validar, también desde el punto de vista costo/beneficio, las orientaciones de seguridad que definirían los requisitos mínimos para la seguridad relativa a los aspectos de las comunicaciones ATM fijas y móviles tales como la arquitectura en tierra y a bordo, redundancia,

conectividad, protección de la información, interoperabilidad, integridad de los datos y aspectos de interferencias.

4. **MEDIDAS PROPUESTAS A LA CONFERENCIA**

4.1 Se invita a la Conferencia a que:

- a) reconozca que las redes fijas y móviles que sirven de soporte para las comunicaciones ATM son “infraestructuras de información crítica” y por lo tanto se deben garantizar las cuestiones de seguridad correspondientes; y
- b) solicite a la OACI que elabore y valide orientaciones para comunicaciones CNI-CII fijas y móviles seguras para ATM prestando atención también a los aspectos costo/beneficios.

— FIN —