



الجمعية العمومية – الدورة الثانية والأربعون اللجنة التنفيذية

البند رقم ١٨ من جدول الأعمال: تنمية القدرات ودعم التنفيذ – السياسة العامة والأنشطة

مقترح لإنشاء برنامج للتدريب في مجال الأمن الإلكتروني
وفقاً للمبادئ التوجيهية الجديدة
(ورقة عمل مقدمة من جمهورية كوريا)

الموجز التنفيذي

يكشف تحليل لإحصائيات الحوادث الإلكترونية الأخيرة في مجال الطيران أن التهديدات الإلكترونية قد تطورت لتصبح خطراً حقيقياً. واستجابةً لذلك، يعمل فريق خبراء الأمن الإلكتروني على وضع إرشادات في هذا الشأن ونشرها، استناداً إلى الفقرة ٩-٤ من الملحق السابع عشر من اتفاقية الطيران المدني الدولي – "أمن الطيران". غير أنه لا تتوفر حالياً سوى دورة تدريبية رسمية واحدة للأمن الإلكتروني تنظمها الإيكاو. ولا بد من إتاحة التدريب والتثقيف لبناء القدرات لمواجهة هذه التهديدات الماثلة. ولذلك، من الضروري تشجيع الدول الأعضاء على إنشاء برامج تدريب تستند إلى إرشادات الأمن الإلكتروني، ويقع على عاتق الإيكاو توحيد هذه الجهود.

الإجراءات: الجمعية العمومية مدعوة إلى:

- أ) إدراك الطبيعة المتطورة للتهديدات الإلكترونية التي تُحدث بالطيران المدني؛
ب) استعراض إرشادات الأمن الإلكتروني المُعدّة بناءً على الشروط الواردة في الفقرة ٩-٤ من الملحق السابع عشر – "أمن الطيران"؛
ج) الشروع في إنشاء برامج تدريب جديدة بقيادة الإيكاو ، بناءً على إرشادات الأمن الإلكتروني المذكورة.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي "ضمان السلامة والأمن لكل رحلة جوية".
الآثار المالية:	من المتوقع أن تنفذ أنشطة الإيكاو المشار إليها في هذه الورقة في حدود الموارد المتاحة في الميزانية العادية للفترة ٢٠٢٦-٢٠٢٨ و/أو من المساهمات الخارجة عن الميزانية وفقاً لخطة أعمال الإيكاو للفترة ٢٠٢٦-٢٠٢٨.
المراجع:	الوثيقة Doc 10184 – "القرارات السارية المفعول الصادرة عن الجمعية العمومية" (في ٢٠٢٢/٧/١٠) ورقة العمل A42-WP/12 – الأمن الإلكتروني في مجال الطيران المدني ورقة العمل A42-WP/13 – "نتائج الشق الوزاري الرفيع المستوى من أسبوع الأمن للإيكاو لعام ٢٠٢٤ الذي انعقد في مسقط بسلطنة عمان"

١ - المقدمة

١-١ في الآونة الأخيرة، تغير هدف الهجمات الإلكترونية. ففي الماضي، كان المهاجمون يركزون على سرقة المعلومات الشخصية، مثل أسماء الركاب وأرقام الهواتف وبطاقات الائتمان. أما الآن، فقد تحول هدفهم إلى التسبب في اضطرابات مباشرة وملموسة في قطاع الطيران المدني، مثل شلّ خدمات النقل الجوي أو تعطيل أنظمة الملاحة الجوية.

٢-١ ووفقاً للبيانات الصادرة عن فريق خبراء التصدي للطوارئ الحاسوبية التابع لإدارة الحركة الجوية الأوروبية (EATM-CERT) للنصف الأول من عام ٢٠٢٥، كان النوع الأكثر شيوعاً من الهجمات الإلكترونية هو برمجيات انتزاع الفدية، التي مثّلت ١٥ حادثاً من أصل ٣٣ (حوالي ٤٥٪)، تلتها عمليات القرصنة بواقع ٧ حالات، ثم هجمات حجب الخدمة الموزع (DDoS) بواقع ٥ حالات. وكانت الجهات المستهدفة الرئيسية هي شركات الطيران، بواقع ١٦ حادثاً (حوالي ٤٨٪)، تليها المطارات بواقع ٧ حوادث، وسلسلة التوريد بواقع ٧ حوادث، وسلطات الطيران المدني بواقع ٣ حوادث.

٣-١ ومن المتوقع أن تستمر هذه الحالات في التزايد. ونظراً للعدد الكبير من الحوادث غير المبلغ عنها، أصبح من الضروري حالياً الاعتراف بأن التهديدات الإلكترونية تشكل خطراً حقيقياً ومثالاً يهدد قطاع الطيران.

٢ - المناقشة

١-٢ تنص الفقرة ٤-٩ من الملحق السابع عشر من اتفاقية الطيران المدني الدولي - "أمن الطيران" على تحديد أنظمة وبيانات تكنولوجيا المعلومات والاتصالات الحيوية المستخدمة لأغراض الطيران المدني، ووضع وتنفيذ التدابير اللازمة لحمايتها من أعمال التدخل غير المشروع، عند الاقتضاء، بناءً على تقييم المخاطر.

٢-٢ وقد استوفت جمهورية كوريا المعايير المطلوبة ذات الصلة العام الماضي من خلال البرنامج العالمي لتدقيق أمن الطيران وفقاً لنهج الرصد المستمر (USAP-CMA) بالنظر إلى لوائحها الوطنية للأمن الإلكتروني، ومن المتوقع أن تتمكن العديد من الدول الأعضاء أيضاً من استيفاء هذه المعايير بشكل كافٍ.

٣-٢ علاوة على ذلك، أعد فريق خبراء الأمن الإلكتروني مؤخراً عدداً من الوثائق الإرشادية وقام بنشرها جزئياً على مدار السنوات الأربع الماضية لتعزيز قدرات الأمن الإلكتروني في مجال الطيران، مما يسهل على الدول الأعضاء تطبيقها في مجال الطيران المدني.

٤-٢ ومن هذا المنظور، يُعتبر أن الوقت بات مناسباً لوضع برنامج الإيكافو للتدريب الخاص بهذه المبادئ التوجيهية بالتوازي. وهناك حاجة إلى وضع برامج تنقيفية وتدريبية تتعلق بالمبادئ التوجيهية للأمن الإلكتروني التي هي إما قيد الإعداد أو نُشرت بالفعل. (يوجد حالياً برنامج واحد يختص بالأمن الإلكتروني تنظمه الإيكافو).

٣ - الخلاصة

١-٣ يُظهر تحليل الإحصاءات من السنوات الخمس الماضية والبيانات الحديثة أنه يجب علينا إدراك أن الوقت قد حان للتأكيد بشكل استباقي على أهمية تعزيز قدرة الأمن الإلكتروني في مجال الطيران على التصدي للهجمات، حيث أصبحت التهديدات الإلكترونية التي تحقق بالطيران المدني حقيقةً ماثلة.

٢-٣ ويجري حالياً إعداد ونشر إرشادات الأمن الإلكتروني التي تتناول التوصيات الواردة في الفقرة ٤-٩ من الملحق السابع عشر - "أمن الطيران"، بقيادة فريق خبراء الأمن الإلكتروني. ومن الضروري أن تتعرف جميع الدول الأعضاء على هذه الإرشادات وأن تقوم بإعداد التدابير لتعديل هيكلها المؤسسي.

٣-٣ ولتحقيق ذلك، تتمثل الحاجة الأكثر إلحاحاً في وضع برامج للتثقيف والتدريب في مجال الأمن الإلكتروني. وعلى الرغم من أن فريق خبراء الأمن الإلكتروني هو الذي يتولى وضع إرشادات التدريب، فإنه لا توجد سوى دورة تدريبية رسمية واحدة من تنظيم الإيكاو. وينبغي أن تشجّع الإيكاو العديد من الدول الأعضاء على وضع برنامج للتدريب في مجال الأمن الإلكتروني ثم العمل على تعميمه.

— انتهى —