



الجمعية العمومية - الدورة الأربعون

اللجنة التنفيذية

البند رقم ١٢ من جدول الأعمال: أمن الطيران - السياسة العامة

الأمن الإلكتروني

(مقدمة من المجلس الدولي للمطارات (ACI))

الموجز التنفيذي

أصبحت التهديدات على أمن الطيران تشكل مخاطر حقيقية بالنسبة للقطاع، ومن المتوقع أن تزداد تلك المخاطر من حيث العدد والتأثير في المستقبل القريب. ولهذا، أضحي من الضروري أن يضع أصحاب الشأن المعنيون بالطيران برنامجاً يضمن قدرة الأمن الإلكتروني على مواجهة المخاطر، مع توفير السبل الرادعة والفعالة للدفاع عن الأمن الإلكتروني. والواقع أن كل مجالات الأعمال، بما في ذلك المطارات، مُعرّضة للخطر الناجم عن التهديدات الإلكترونية، سواء كان لدى تلك الأعمال نظم إلكترونية بسيطة أو برامج التحول الرقمي لتكنولوجيا المعلومات الأكثر تعقيداً.

وثمة حاجة واضحة للتعاون الدولي والتنسيق بين نظم الإدارة والسياسات المتسقة والعملية لتناول مسألة الأمن الإلكتروني، مقترنةً بحلول عملية لتبادل المعلومات والمراقبة وبناء القدرات والتدريب. ولا يجدي النهج المنعزل في التعامل الفعال لهذه المسألة؛ بل ما نحتاج إليه هو الرؤية والاستراتيجية الواضحة لمنظمة الطيران المدني الدولي (الإيكاو) والعمل المشترك بين مختلف التخصصات الذي يغطي أوجه السلامة والأمن والعمليات والصمود في مواجهة المخاطر.

الإجراء: الجمعية العمومية مدعوة إلى:

- أ) دعم استراتيجية الإيكاو في مجال الأمن الإلكتروني، والطلب إلى الإيكاو أن تعمل مع الدول وقطاع الطيران على بلورة خطة عمل دعماً لتلك الاستراتيجية؛
- ب) الاعتراف بالحاجة الملحة إلى نهج متعدد التخصصات للتعامل مع الأمن الإلكتروني؛
- ج) الطلب إلى الإيكاو الاستكمال السريع لعملية تقييم هيكل نظم الإدارة الراهن للأمن الإلكتروني، مع النظر الجاد في تشكيل فريق يُعنى بمسائل الأمن والسلامة والصمود في مواجهة المخاطر واستمرارية العمليات؛ على أن يتشكل هذا الفريق من متخصصين أكفاء من الدول وقطاع الطيران، بهدف إحراز التقدم في العمل الذي تحدده "استراتيجية الأمن الإلكتروني". ولابد للفريق أن يعمل تحت الإدارة المشتركة للجنة الملاحة الجوية وأي من لجنة الأفعال غير المشروعة أو لجنة النقل الجوي؛
- د) الطلب إلى الإيكاو إشراك قطاع الطيران والدول عند وضع السياسات والاستراتيجيات والخطط والقواعد الخاصة بالأمن الإلكتروني في مجال الطيران.

¹ نسخ باللغة العربية والإنجليزية والصينية والفرنسية والروسية والإسبانية مقدمة من (ACI).

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالأهداف الاستراتيجية التالية: السلامة، وسعة وكفاءة الملاحة الجوية، والأمن والتسهيلات.
الآثار المالية:	سنتفد الأنشطة المشار إليها في ورقة العمل هذه باستخدام الموارد المتاحة في ميزانية البرنامج العادي للفترة ٢٠٢٠-٢٠٢٢، و/أو المساهمات من خارج الميزانية الاعتيادية.
المراجع:	ورقة عمل الجمعية العمومية (A40-WP/28 EX/13) - استراتيجية الإيكاو في مجال الأمن الإلكتروني الملحق السابع عشر - الأمن، الوثيقة (Doc 8973) - دليل أمن الطيران

١- المقدمة

١-١ أضحى نظم الطيران أكثر ترابطاً فيما بينها، حيث أصبح هناك اعتماد متبادل بين نظم المطارات، ومشغلي الطائرات، ومقدمي خدمات الملاحة الجوية (ANSPs)، والمناولين الأرضيين، ونظم الركاب، في تبادل المعلومات الرقمية.

٢-١ وقد أصبحت التهديدات على أمن الطيران تشكل مخاطر حقيقية بالنسبة للقطاع، ومن المتوقع أن تزداد تلك المخاطر من حيث العدد والتأثير في المستقبل القريب. ولهذا، أضحي من الضروري أن يوفر أصحاب الشأن المعنيون بالطيران السبل الرادعة والفعالة للدفاع عن الأمن الإلكتروني، مع وضع برنامج يضمن قدرة الأمن الإلكتروني على مواجهة المخاطر. والواقع أن كل مجالات الأعمال، بما في ذلك المطارات، مُعرّضة للخطر الناجم عن التهديدات الإلكترونية، سواء كان لدى تلك الأعمال نظم إلكترونية بسيطة أو برامج التحول الرقمي لتكنولوجيا المعلومات الأكثر تعقيداً.

٣-١ ومن الأهمية البالغة التأكيد على أن الأمن الإلكتروني ليس مسألة تتعلق "فقط" بتكنولوجيا المعلومات والاتصالات. فالأمن الإلكتروني هو مسؤولية مؤسسية عامة، حيث يعتمد الصمود في مواجهة المخاطر الإلكترونية بشكل فعال على دعم الجميع، والضمان الصارم للجودة والرقابة، والأطر السياسية الواضحة، والتعاون الناجع بين أصحاب الشأن. وإنه لمن الضروري تطوير ثقافة أمن المعلومات في قطاع الطيران.

٤-١ يمكن للتهديدات والوقائع المتعلقة بالأمن الإلكتروني أن تؤثر على نظام النقل الجوي برمته، كما يمكن أن تثير عدداً من الشواغل الخاصة بالسلامة وتلك الخاصة بالأمن، إضافةً إلى انقطاع العمليات والخسارة المالية، مما يؤدي إلى تبعات تعبر الحدود بسرعة ويكون لها أثر عالمي.

٥-١ يُعتبر فهم تهديدات الأمن الإلكتروني عاملاً حاسماً لفهم وإدارة المخاطر. ومن الضروري أن يتعاون الجميع في قطاع الطيران من أجل تعزيز الحوار القائم على تقدير أوجه النظر المتعددة والاتفاق على مجموعة من الإجراءات المشتركة.

٦-١ تشكلت لدى صناعة الطيران خبرة عقود في معالجة المسائل المتعلقة بالسلامة والأمن، إلا أن الأمن الإلكتروني يُعد تحدياً جديداً نسبياً. وتمضي صناعة الطيران والمطارات في اكتساب الخبرة في معالجة مخاطر الأمن الإلكتروني. ولهذا الغرض، لابد من الارتباط المتساوي بين الصناعة والدول في اتخاذ القرارات، وفي بلورة السياسات والقواعد في أجهزة الإيكاو المعنية. وقد يأخذ الأمر وقتاً أطول لوضع واستبدال نظم الطيران عما يتطلب تطوير قدرات مقترفي التهديدات؛ وعليه، ثمة حاجة لنهج يُمكن الصناعة من الاستمرار في تطبيق الممارسات الفضلى وفقاً للقواعد العالمية الراهنة مثل الأيزو (ISO)، مع الترويج للمزيد من التطبيق عالمياً.

٧-١ وهناك احتياج لنهج شامل يتناول أمن وسلامة وقدرة نظام النقل الجوي على الصمود وتدابير الحماية وآليات الاستجابة وتبادل المعلومات وبناء القدرات والمراقبة.

٢- المناقشة

١-٢ عالجت الإيكاو الأمن الإلكتروني والقدرة على الصمود في وجه الهجمات على الأمن الإلكتروني في محافل مختلفة خلال السنوات الماضية الأخيرة.

٢-٢ ويتناول الفريق المعني بأمن الطيران (AVSEC) حالياً مسألة الأمن الإلكتروني من منظور أمن الطيران، حيث ركز أساساً على استخدام أمن الطيران بغرض إرهابي للإضرار بالطيران. وقد عالجت ثلاث مجموعات عمل منبثقة عن الفريق هذه المسألة بالتفصيل.

٣-٢ أجرت مجموعة عمل التهديدات والمخاطر (في عام ٢٠١٥) تحليلاً لخطر حدوث هجوم مُتعمد على الأمن الإلكتروني قد يؤثر على نظم شركات الطيران والمطارات والملاحة الجوية. وقد تم التركيز، بالنسبة للمطارات بالذات، على التلاعب بنظم الأمن مثل نظم ضوابط الدخول، ومعدات التفتيش الأمنية.

٤-٢ وقد أعدت مجموعة عمل المواد الإرشادية (WGGM) التابعة للفريق المعني بأمن الطيران (AVSEC) فصلاً خاصاً عن الأمن الإلكتروني في "دليل الأمن" الصادر عن الإيكاو (الوثيقة 8973 Doc). ويغطي هذا الفصل، على مستوى عالٍ، خلفية عامة للدول وإرشادات بشأن تقييم المخاطر ووضع سياسة لمعالجتها وإطاراً مقترحاً ونظم الإدارة والتدريب وممارسات التصميم والمشتريات والاكتشاف والاستجابة للوقائع والتعافي منها والإبلاغ.

٥-٢ وقد ناقشت مجموعة عمل الملحق السابع عشر التابعة للفريق المعني بأمن الطيران (AVSEC) القواعد والتوصيات الدولية (SARPs) مطولاً؛ مما أفضى إلى دعم الفريق آنذاك لتوصيتين في التعديل الخامس عشر للملحق السابع عشر، تم استبدالهما بقاعدة وتوصية متضمنتين في التعديل السادس عشر للملحق السابع عشر في نوفمبر ٢٠١٨.

٦-٢ في إطار دراسة إمكانية توفير شبكة موثوق فيها للملاحة الجوية، شكلت الأمانة العامة للإيكاو فريق "إنوفا" "INNOVA" ضمن إدارة الملاحة الجوية، وذلك بهدف تيسير تبادل المعلومات بأمان وقدرة على الصمود، وسلاسة، في بيئة الاتصال الرقمي دعماً للعمليات الحالية والمستقبلية. ولتنفيذ هذا الهدف، أنشئ مجموعة دراسة الإطار الاستئماني (TFSG) ضمن إدارة الملاحة الجوية لوضع مجموعة مشتركة من المبادئ والسياسات والإرشادات، بالإضافة إلى استراتيجية انتقالية نحو إطار عالمي موحد يسمح لأصحاب الشأن في قطاع الطيران بتبادل البيانات والمعلومات أرض-أرض، وجو-جو الموثوق فيها، وذلك بالدرجة المطلوبة من الصمود في مواجهة المخاطر وقابلية التشغيل المشترك لدعم زيادة السعة والكفاءة في للعمليات التشغيلية المتواصلة والأمنة لمنظومة الطيران المدني.

٧-٢ كما أنشأت الإيكاو مجموعة الدراسة التابعة للأمانة العامة بشأن الأمن الإلكتروني (SSGC) برئاسة نائب المدير لشؤون أمن الطيران والتسهيلات (DD/ASF)، التي عكفت على إعداد توصيات للإيكاو بشأن الاستراتيجية، والسياسة القانونية، والاحتياجات العامة للدول والصناعة فيما يتعلق بالأمن الإلكتروني؛ ولكن المجموعة محدودة من حيث النطاق والمشاركة.

٨-٢ وقد وضع فريق خبراء نظم الطائرات الموجهة عن بُعد (RPAS) قواعد لتبادل المعلومات بين الطائرات الموجهة عن بُعد ومحطات القيادة عن بُعد من أجل تخفيض احتمال أي تحكّم غير مرخص، والتخفيف من آثارها.

٩-٢ وتقوم الإدارة القانونية بالنظر في مدى كفاية صكوك القوانين الجوية الدولية الحالية في معالجة التهديدات الإلكترونية ضد الطيران المدني.

١٠-٢ يعترف المجلس الدولي للمطارات باعتبار الإيكاو المنظمة الأنسب لدفع عمل قطاع الطيران في مجال الأمن الإلكتروني إلى الأمام. إلا أن تقسيم الأنشطة الخاصة بالأمن الإلكتروني داخل الإيكاو كما هو مشار إليه أعلاه، لا يسمح بالعمل وفق نهج فعال وشامل.

١١-٢ لا يرى المجلس الدولي للمطارات ضرورة لوضع قواعد مفصلة أو وصفية للأمن الإلكتروني، بل قد تؤدي تلك القواعد إلى نتيجة عكسية بما أن هذه المسألة تتميز بسرعة وتيرتها وتقلبها، مما يتطلب الاستجابة المرنة والسريعة. والدول على اختلافها، لديها نُهج مختلفة، وعليها مسؤوليات تتفاوت بين وكالة وأخرى. وهذا ما يجعل من الصعب والمعقد تطبيق مجموعة من القواعد الخاصة بقطاع الطيران وحده.

١٢-٢ إلا أن ثمة حاجة واضحة للتعاون الدولي والتنسيق بين نظم الإدارة والسياسات المتسقة والعملية لتناول تلك المسائل، مقترنةً بحلول عملية لتبادل المعلومات والمراقبة وبناء القدرات والتدريب. كما أن هناك حاجة ملحة لوضع استراتيجية وخطة عمل للطيران المدني.

١٣-٢ ولا بد لخطة العمل هذه أن تعزز وتيسر بلورة مبادئ توجيهية وقواعد ومقاييس مشتركة وتبادل الوعي والمعرفة بالأمن الإلكتروني لمنظومة الطيران. وإضافة إلى ذلك، لا بد من دعم مبادرات إكفاء الوعي وتشارك أصحاب الشأن في الدراية التقنية والممارسات، بهدف تعظيم الاستفادة بالدروس المستفادة والممارسات الفضلى.

٣- الخلاصة

١-٣ يؤيد المجلس الدولي للمطارات بالكامل ورقة العمل المُعدّة من قبل الأمانة العامة للإيكاو حول استراتيجية الأمن الإلكتروني، وسيستمر المجلس في لعب دور نشط في تطويرها وتطبيقها.

٢-٣ من بالغ الأهمية أن تُسرّع الإيكاو والدول والصناعة من العمل في هذا المجال، والعمل سويًا في كافة التخصصات من أجل معالجة الأمن الإلكتروني. وهي مسألة لا يمكن أن تُقسّم تلقائياً إلى جوانب تتعلق بالسلامة أو الأمن أو العمليات أو الملاحة الجوية أو التسهيلات، بل هي مسألة تشمل كل المجالات؛ حيث يندرج تقييم المخاطر والمواد الإرشادية ووضع السياسات والمراقبة ضمن تلك المجالات.

٣-٣ والفريق المعني بالأمن الإلكتروني، إذا توفرت فيه الموارد المطلوبة، قد يستطيع معالجة بعض المسائل المحددة أعلاه، من خلال:

- أ) نطاق أوسع من التخصص والخبرة بين أعضاء الفريق، خاصةً فيما يتعلق بالأمن الإلكتروني؛
- ب) نهج شامل عند تقييم المخاطر، مع تطبيق منهجيات متفق عليها ومفهومة من قبل كل أصحاب الشأن، والاستفادة من الخبرة الإقليمية والوطنية؛
- ج) القدرة على تشكيل مجموعات عمل من أجل تكريس مزيد من الوقت والموارد لإعداد مواد إرشادية وبرامج، وتعزيز بناء القدرات والمساعدة والتدريب، حسبما يكون ذلك ضرورياً؛
- د) والنظر في مسائل الملاحة الجوية والسلامة والأمن معاً من خلال جهة واحدة.

- انتهى -