



المؤتمر الرابع عشر للملاحة الجوية

مونتريال، كندا، من ٢٦/٨/٢٠٢٤ إلى ٦/٩/٢٠٢٤

البند ٤ من جدول الأعمال: الترابط الفائق في شبكة الملاحة الجوية
٢-٤: الأمن الإلكتروني وقدرة نظام المعلومات على الصمود

تنفيذ العناصر الأساسية التي يتكون منها الإطار العام للأمن الإلكتروني بقطاع الطيران

(مقدمة من الأمانة العامة)

الموجز التنفيذي

إن التحوّل الرقمي الذي شهده قطاع الطيران المدني في جميع مجالات الطيران يجعل الحاجة إلى معالجة مسألة الأمن الإلكتروني في الطيران المدني لضمان سلامة القطاع وأمنه وسعته وكفاءته. فتعرض هذه الورقة عدداً من العناصر الأساسية الرفيعة المستوى التي ينبغي أن تنتظر فيها الدول والجهات المعنية لمعالجة الأمن الإلكتروني في قطاع الطيران بطريقة شاملة ومنسقة في جميع المجالات ذات الأهمية. كما تُبرز الورقة الحاجة إلى قيام الإيكاو بإعداد إرشادات إضافية لدعم الدول والجهات المعنية بقصد تعزيز حماية القطاع وقدرته على الصمود في مواجهة التهديدات والمخاطر الإلكترونية. كما تطرح الورقة توصيات تسمح بمزيد من المواءمة والاتساق على الصعيد الإقليمي.

الإجراءات: يُدعى المؤتمر إلى الموافقة على التوصية ٢-٤/.. - "الأمن الإلكتروني في قطاع الطيران" الواردة في الفقرة ٣.

الأهداف الاستراتيجية	تتعلق هذه الورقة بالأهداف الاستراتيجية: "السلامة" و"سعة وكفاءة الملاحة الجوية" و"الأمن والتسهيلات".
الأثار المالية	الأثر على أوساط الطيران: ستكون هناك تكاليف تنشأ عن تنفيذ الجوانب التي تتناولها هذه الورقة. إلا أن هذا التنفيذ سيُتيح الفرصة لاتباع نهج واضح فيما يخص الأمن الإلكتروني في قطاع الطيران، على أساس أدوار ومسؤوليات محددة جيداً بالنسبة لجميع الجهات المعنية بالمسألة.

الأثر على الإيكاو (مقارنة بالمستويات الحالية من موارد ميزانية البرنامج العادي): ستستمر أنشطة الإيكاو المشار إليها في ورقة العمل هذه خلال الفترة الثلاثية القادمة. وستكون هناك حاجة إلى موارد إضافية للقيام بهذه الأنشطة فضلاً عن القيام بحملات توعية وتقديم الدعم للتنفيذ.	
"دليل أمن الطيران" (Doc 8973، مقيد التوزيع) "الخطة العالمية للملاحة الجوية" (Doc 9750) "الخطة العالمية للسلامة الجوية" (Doc 10004) "الخطة العالمية لأمن الطيران" (Doc 10118) "القرارات السارية المفعول الصادرة عن الجمعية العمومية (في ٢٠٢٢/١٠/٧)" (Doc 10184) استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران خطة عمل الأمن الإلكتروني إرشادات سياسة الأمن الإلكتروني ثقافة الأمن الإلكتروني في الطيران المدني	المراجع

١- المقدمة

١-١ أعادت الجمعية العمومية للإيكاو التأكيد أثناء دورتها الأربعين على الأهمية والطابع الملح للالتزام العالمي بالعمل بشكل تعاوني من جانب جميع الجهات المعنية لمعالجة الأمن الإلكتروني في مجال الطيران المدني، وذلك باعتماد القرار ٤٠-١٠: "معالجة الأمن الإلكتروني في الطيران المدني" وإقرار "استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران".^١ وأكدت الجمعية العمومية للإيكاو مجدداً في دورتها الحادية والأربعين على أهمية معالجة الأمن الإلكتروني في مجال الطيران المدني من خلال القرار المحدث ٤١-١٩.

٢-١ ودعت الجمعية العمومية أيضاً الإيكاو إلى وضع خطة عمل لدعم الدول والجهات المعنية في تنفيذها لاستراتيجية الأمن الإلكتروني في مجال الطيران. وتتضمن الطبعة الثانية من خطة عمل الأمن الإلكتروني^٢، التي نُشرت في يناير ٢٠٢٢، الأساس الذي يتيح للإيكاو والدول والجهات المعنية للعمل معاً، وتُقرّح أيضاً سلسلة من المبادئ والتدابير والإجراءات لتحقيق الغايات المنشودة من الركائز السبع لاستراتيجية الأمن الإلكتروني^٣.

٣-١ وتمشياً مع خطة عمل الأمن الإلكتروني، نشرت الإيكاو بالفعل مواداً إرشادية بشأن موضوعات عن الأمن الإلكتروني في قطاع الطيران. وشمل عمل الإيكاو أيضاً مبادرات تتعلق بالبحث في مدى كفاية الوثائق القانونية الدولية للتصدي للهجمات الإلكترونية ضد الطيران المدني، والبحث في مدى الحاجة إلى تضمين الملاحق باتفاقية الطيران المدني الدولي (اتفاقية شيكاغو) قواعد وتوصيات دولية تعالج موضوع الأمن الإلكتروني، وإعداد مواد لإرساء الثقة في إمكانية التشغيل البيئي في مختلف مجالات الطيران، ورفع مستوى الوعي بأهمية التصدي للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني، وتطوير مبادرات بناء القدرات في مجال الأمن الإلكتروني للطيران، وإجراء تمارين بالحاكاة على جوانب الأمن الإلكتروني في الطيران الدولي.

^١ <https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx>

^٢ <https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx>

^٣ تتمثل ركائز استراتيجية الإيكاو للأمن الإلكتروني للطيران فيما يلي: التعاون الدولي ونظم الإدارة والتشريعات واللوائح الفعالة وسياسة الأمن الإلكتروني وتبادل المعلومات وإدارة الحوادث والتخطيط للطوارئ وبناء القدرات والتدريب، وثقافة الأمن الإلكتروني.

٢- المناقشة

١-٢ بينما يواصل قطاع الطيران المدني الاستفادة من الابتكارات التكنولوجية لتعزيز سعته وكفاءته، مع الحفاظ على مستويات السلامة والأمن المتفق عليها، يجري النظر في الأمن الإلكتروني في كل مجال من مجالات الطيران على حدة. وقد أدى ذلك على مر السنين إلى أن أصبح الطيران منظومةً تضم أنظمةً عدة، إذ أن ضوابط وعمليات حماية الأمن الإلكتروني والقدرة على الصمود في وجه الأزمات لم تُصمم ولم يتم تنفيذها بشكلٍ كليٍّ شامل، مما أدى إلى وجود فجوات محتملة على المستوى الكلي.

٢-٢ ومن هذا المنطلق، من المهم إدماج منظور الأمن الإلكتروني للطيران في مجالات الطيران المدني على المستويات الوطنية والإقليمية والدولية بطريقة منسقة ومتوافقة وشاملة. وهذا من شأنه أن ييسر التصدي للتهديدات والمخاطر الإلكترونية على الطيران المدني، دون تعريض متطلبات السلامة والأمن والسعة والكفاءة للخطر.

٣-٢ وقد أُحرز تقدم كبير في معالجة الأمن الإلكتروني في الطيران المدني، ولكن هناك حاجة إلى إرشادات إضافية لتسهيل قيام الدول بإدراج مسائل الأمن الإلكتروني في لوائحها التنظيمية والرقابية الموجودة بالفعل، وكذلك في خططها الإقليمية والوطنية المتصلة بمجالات الطيران المدني المعنية، وأهمها السلامة الجوية وأمن الطيران والتسهيلات والملاحة الجوية.

٤-٢ وعلاوة على ذلك، يشدد كل من قرار مجلس الأمن التابع للأمم المتحدة رقم ٢٣٤١ (٢٠١٧) بشأن حماية البنى الأساسية الحيوية من الأعمال الإرهابية، وقرار الجمعية العامة للأمم المتحدة (A/RES/77/298) بشأن الاستعراض الثامن لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/RES/60/288)، على أهمية التعاون المتعدد الجهات والشامل لمختلف المجالات من أجل معالجة الأمن الإلكتروني في المنظمات الإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدني.

٥-٢ ومن ثم، وتمشياً مع القرارات السارية الصادرة عن الجمعية العمومية للإيكاو، واستراتيجية الأمن الإلكتروني للطيران وخطة عمله، ومختلف المواد الإرشادية التي أعدتها الإيكاو، تقترح هذه الورقة مجموعةً أوليةً مبسطة من العناصر الأساسية التي ينبغي أن تنتظر فيها الدول والجهات المعنية للتصدي للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني. وينبغي أن تشمل هذه العناصر الأساسية ما يلي:

أ) الجوانب التنظيمية على مستوى الدولة:

١- **نُظُم إدارة الأمن الإلكتروني في الطيران على مستوى الدولة:** يشمل هذا العنصر، على سبيل المثال لا الحصر، الجوانب المتعلقة بتحديد سلطة تختص بالأمن الإلكتروني للطيران، وإدراج الأمن الإلكتروني للطيران في برامج السلامة والبرامج الوطنية لأمن الطيران المدني لدى الدول، وتحديد أدوار ومسؤوليات سلطات الطيران والسلطات الأخرى (مثل سلطات الأمن الإلكتروني الوطنية) وتنسيق أنشطتها فيما يتعلق بتنظيم ومراقبة الأمن الإلكتروني في الطيران المدني، والاستفادة من موارد الأمن الإلكتروني الوطنية لدعم المنظمات في أنشطة مراقبة الوقائع الإلكترونية واكتشافها والاستجابة لها والتعافي منها.

٢- **الإطار القانوني الوطني:** يشمل هذا العنصر الجوانب المتعلقة بالأطر القانونية الوطنية لدى الدول للسماح برفع الدعاوى القضائية في حالة شن هجمات إلكترونية ضد الطيران المدني. ويشمل أيضاً الجوانب المتعلقة بالتصديق على اتفاقية قمع الأعمال غير المشروعة المتعلقة بالطيران المدني الدولي (بيجين، ٢٠١٠) والبروتوكول المُكَمَّل لاتفاقية قمع الاستيلاء غير المشروع على الطائرات (بيجين، ٢٠١٠) كوسيلة للتعامل مع الهجمات الإلكترونية ضد الطيران المدني على الصعيد العالمي.

٣- سياسات الأمن الإلكتروني في مجال الطيران: يشمل هذا العنصر الجوانب المتعلقة بسياسة الأمن الإلكتروني في مجال الطيران على مستوى الدولة.

٤- المهام الرقابية: يشمل هذا العنصر الجوانب المتعلقة بالمهام الرقابية التي تضطلع بها الدول في مجال الأمن الإلكتروني للطيران، والتي يمكن تنفيذها بشكل منسق بواسطة الآليات الموجودة بالفعل لمراقبة السلامة الجوية وأمن الطيران.

(ب) الجوانب ذات الصلة بالدول والجهات المعنية:

١- إدارة المخاطر الإلكترونية: يشمل هذا العنصر الجوانب المتعلقة بتحديد البنية الأساسية الحيوية للطيران وإدراج تقييم المخاطر الإلكترونية في التقييمات الحالية لمخاطر السلامة والأمن بالنسبة لتلك البنية الأساسية.

٢- الإبلاغ عن الوقائع الإلكترونية: يشمل هذا العنصر الجوانب المتعلقة بإنشاء آلية تتيح لمختلف الهيئات إبلاغ السلطات التي تتبعها بالوقائع الإلكترونية، وهو ما يمكن القيام به إما بصورة منفصلة أو من خلال آليات الإبلاغ الحالية المستخدمة في مجالات السلامة الجوية أو أمن الطيران.

٣- تبادل المعلومات الإلكترونية: يشمل هذا العنصر الجوانب المتعلقة بإنشاء آليات لتبادل المعلومات بين الدول والجهات المعنية على المستويات الوطنية والإقليمية والدولية.

٤- التصدي للوقائع الإلكترونية والتعافي منها: يتضمن هذا العنصر الجوانب المتعلقة بتنفيذ خطط وإمكانيات التصدي للوقائع الإلكترونية والتعافي منها. ويشمل أيضاً الجوانب المتعلقة بإدماج تلك الخطط في خطط الاستجابة لحالات الطوارئ/إدارة الأزمات في مجال الطيران.

٥- إدارة سلاسل الإمداد الإلكترونية: يتضمن هذا العنصر الجوانب المتعلقة بإدارة المخاطر الإلكترونية الناجمة من سلاسل الإمداد الجوية وغير الجوية. ويشمل ذلك عدة أنواع من سلاسل الإمداد، مثل المعدات/الأنظمة المعتمدة للطيران، وخدمات أنظمة الطيران (مثل أنظمة تخطيط الرحلات الجوية، وشبكات المطارات)، ومقدمي الخدمات غير الجوية (مثل مقدمي الخدمات السحابية، ومقدمي خدمات الاتصالات الساتلية).

٦- ثقافة الأمن الإلكتروني: يشمل هذا العنصر الجوانب المتعلقة بإرساء ثقافة قوية للأمن الإلكتروني في الطيران المدني، تستفيد من خبرة القطاع في إرساء ثقافات السلامة والأمن.

٧- برامج التدريب على الأمن الإلكتروني للطيران: يشمل هذا العنصر الجوانب المتعلقة بإعداد ونشر برامج التدريب على الأمن الإلكتروني في مجال الطيران المصممة لمختلف فئات المتلقين (مثل التوعية العامة مقابل التدريب القائم على الأدوار).

٦-٢ وبالنظر إلى أن قطاع الطيران يُصنّف ضمن البنى الأساسية الوطنية ذات الأهمية الحرجة في العديد من الدول، فمن الضروري وضع نهج تدريجي ومتعدد المستويات لمعالجة مسألة حماية الأمن الإلكتروني في القطاع وقدرته على الصمود

في وجه الأزمات. والهدف هو وضع استراتيجية 'الدفاع في العمق' بحيث تشمل جميع الجهات المعنية المشاركة بشكل مباشر أو غير مباشر في معالجة التهديدات والمخاطر الإلكترونية على الطيران المدني. ولا تشكل العناصر المبينة أعلاه القائمة الكاملة للمجالات التي ينبغي تناولها في نطاق الأمن الإلكتروني في مجال الطيران؛ بل يمكن اعتبارها الأساس الذي يسمح بإدارة قوية وفعالة للأمن الإلكتروني في مجال الطيران، بما في ذلك حماية أصول الطيران التي تديرها الدول والجهات المعنية وإكسابها القدرة على مواجهة الأزمات.

٧-٢ يجري إنشاء أفرقة للأمن الإلكتروني في مختلف أقاليم الإيكاو لدعم المناقشات الإقليمية عن موضوع حماية الأمن الإلكتروني والقدرة على الصمود في مختلف مجالات الطيران. وتُعد هذه الأنشطة وثيقة الصلة بمعالجة مجالات محددة تتعلق بكل إقليم بعينه فيما يخص التهديدات والمخاطر الإلكترونية، ومع ذلك، فهناك خطر محتمل يتمثل في التكرار أو ربما حتى التعارض إذا لم يتم التنسيق بين هذه الأنشطة عبر المجموعات والخطط الإقليمية المختلفة. وسيسمح هذا التنسيق باتباع نهج شامل ومنسق ومتوافق للتصدي للتهديدات والمخاطر الإلكترونية في مختلف الأقاليم، كما سيضمن الاتساق والتكامل في الخطط الإقليمية للملاحة الجوية والسلامة والأمن والتسهيلات من حيث مسائل الأمن الإلكتروني في الطيران، مما سيؤثر بشكل إيجابي على أنشطة التخطيط والتنفيذ التي تضطلع بها الدول الأعضاء على المستويات الوطنية. ويمكن للدول أيضاً أن تستخدم هذه المنتديات لإطلاع الإيكاو على التحديات التي تواجهها في معالجة الأمن الإلكتروني في مجال الطيران المدني لديها، وهو ما ستسترشد به الإيكاو في أنشطتها المتعلقة بوضع الأحكام وإعداد المواد التوجيهية.

٣- الخلاصة

١-٣ يبرز التحول الرقمي الذي تشهده جميع مجالات الطيران في قطاع الطيران المدني الحاجة إلى معالجة الأمن الإلكتروني في الطيران المدني لضمان سلامة القطاع وأمنه وسعته وكفاءته. ومع التسليم بالتحديات المرتبطة بالأمن الإلكتروني للطيران، ينبغي على الدول والجهات المعنية النظر في المجموعة الأولية المبسطة من العناصر الأساسية على المستويين التنظيمي والتشغيلي.

٢-٣ وعلى ضوء ما تقدم، فإن المؤتمر مدعو إلى الموافقة على التوصية التالية:

التوصية ٤-٢/.. - الأمن الإلكتروني في مجال الطيران

أن تقوم الدول بما يلي:

أ) وضع وتنفيذ خطة وطنية للتصدي بشكل شامل للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني في جميع مجالات الطيران، بالتنسيق مع الجهات المعنية بهذا الشأن من خارج قطاع الطيران باستخدام العناصر الأساسية كمرجع؛

ب) التوفيق بين أنشطة الأمن الإلكتروني في مجال الطيران ضمن الخطط الإقليمية للملاحة الجوية والسلامة والأمن والتسهيلات من خلال عمليات المجموعات الإقليمية للتخطيط والتنفيذ (PIRGs) والمجموعات الإقليمية للسلامة الجوية (RASGs) والمجموعات الإقليمية المعنية بأمن الطيران والتسهيلات (AVSEC/FAL)؛

^٤ يُقصد بالدفاع في العمق تطبيق تدابير مضادة متعددة بطريقة متعددة الطبقات أو تدريجية لتحقيق الأهداف الأمنية. وتتضمن المنهجية الاعتماد على طبقات من التكنولوجيات الأمنية المتباينة غير المتجانسة في ناقلات الهجوم الشائعة لضمان كون الهجمات التي غفلت عنها تقنية ما سيتم اكتشافها بواسطة تقنية أخرى (انظر ISO/IEC 62443 1-1).

ج) إطلاع الإيكاو على تجربتها في تنفيذ أحكام الإيكاو والمواد الإرشادية المتعلقة بالأمن الإلكتروني في مجال الطيران، من خلال أفرقة الخبراء المختصة أو من خلال عمليات المجموعات الإقليمية للتخطيط والتنفيذ (PIRGs) والمجموعات الإقليمية للسلامة الجوية (RASGs) والمجموعات الإقليمية المعنية بأمن الطيران والتسهيلات (AVSEC/FAL)؛

أن تقوم الإيكاو بما يلي:

د) تقديم إرشادات بشأن العناصر الأساسية لدعم الدول والجهات المعنية في معالجة الأمن الإلكتروني في مجال الطيران، وتحقيق التكامل بين جميع أنشطة الأمن الإلكتروني للطيران بشكل كلي شامل وبطريقة منسقة ومنسقة.

— انتهى —