



الجمعية العمومية - الدورة الثانية والأربعون

اللجنة التنفيذية

البند رقم ١٣ من جدول الأعمال: الأمن الإلكتروني-السياسات العامة

الممارسات والتحسينات الراهنة في مجال الأمن الإلكتروني للطيران المدني الدولي

(ورقة مقدمة من السلفادور بالنيابة عن الدول الأعضاء في هيئة أمريكا الوسطى لخدمات الملاحة الجوية^٢ (COCESNA))

الموجز التنفيذي

تؤدي التكنولوجيا دوراً حيوياً في قطاع الطيران، حيث تسهل السياحة والتجارة والربط العالمي وتدفع عجلة النمو الاقتصادي وتحسن جودة الحياة. وقد مكّنت التطورات التي شهدتها إلكترونيات الطيران من تحقيق تحسينات هامة على صعيد إدارة الملاحة الجوية وسلامة الطائرات والكفاءة التشغيلية. ويعد الابتكار التكنولوجي في هذا القطاع أمراً أساسياً للحفاظ على القدرة التنافسية والاستجابة للطلبات المتزايدة على النقل الجوي.

أصبح الأمن الإلكتروني في مجال الطيران المدني حجر الزاوية لضمان السلامة وكفاءة الملاحة الجوية. ويواجه القطاع حالياً بيئة متغيرة في ظل تهديدات إلكترونية متطورة باستمرار، مما يتطلب نهجاً استراتيجياً ومنسقاً لضمان حماية البنى الأساسية الحيوية. تقدم ورقة العمل هذه تحليلاً للممارسات الحالية الخاصة بالأمن الإلكتروني في صناعة الطيران وتقدم الجوانب الرئيسية التي ينبغي مراعاتها من أجل تحسينها وتنفيذها مستقبلياً، وذلك بهدف تعزيز تحسين أنظمة الطيران أمام التهديدات الإلكترونية الناشئة.

الإجراءات: يُرجى من الجمعية العمومية القيام بما يلي:

- الإحاطة علماً بالمعلومات الواردة؛
- الطلب من الإيكاو تقييم استراتيجيات الأمن الإلكتروني وتعزيزها واعتماد منهجيات قائمة على أفضل الممارسات الدولية وتبادل المعلومات والتكنولوجيات الجديدة؛
- الطلب من الإيكاو مواصلة دعم الدول الأعضاء في وضع وتنفيذ الأطر التنظيمية للأمن الإلكتروني، فضلاً عن تدريب الموظفين في هذا المجال وتعزيز كفاءاتهم وإنشاء خطط للمرونة الإلكترونية ترمي إلى إدراج الأمن الإلكتروني في الخطط الوطنية للسلامة الجوية (NASPs).

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالأهداف الاستراتيجية: "ضمان سلامة وأمن كل رحلة جوية" "عدم ترك أي بلد وراء الركب" "التممية الاقتصادية للنقل الجوي تضمن تحقيق الازدهار الاقتصادي والرفاه المجتمعي للجميع"
-----------------------	--

^١ قدمت السلفادور النسخة باللغة الإسبانية

^٢ بيليز وكوستاريكا والسلفادور وغواتيمالا وهندوراس ونيكاراغوا

الآثار المالية:	
المراجع:	الإطار التنظيمي للمعهد الوطني للمعايير والتكنولوجيا (NIST) الوثيقة (Doc 9985) - "دليل أمن إدارة الحركة الجوية" الوثيقة (Doc 10075) - "قرارات الجمعية العمومية سارية المفعول (في ٢٠١٦/١٠/٦)" الوثيقة (Doc 10161) - "خريطة الطريق العالمية للسلامة الجوية" الملحق السابع عشر - "أمن الطيران"

١- المقدمة

١-١ تؤدي التكنولوجيا دوراً حيوياً في قطاع الطيران، حيث أثمرت التطورات التكنولوجية عن منافع هامة في تقديم خدمات الملاحة الجوية. وقد غيّرت أنظمة مثل الملاحة القائمة على الأداء (PBN) وإذاعة الاستطلاع التابع التلقائي (ADS-B) وإدارة الحركة الجوية (ATM) الطريقة التي تُدار بها الرحلات، الأمر الذي حسن الدقة والسلامة والكفاءة. وتتيح هذه الأنظمة تحسين تخطيط الطرق الجوية وتقليل التأخيرات وتحسين استخدام المجال الجوي.

٢-١ بات الأمن الإلكتروني في مجال الطيران المدني أمراً بالغ الأهمية، إذ تعتمد العمليات بشكل متزايد على أنظمة رقمية مترابطة تُعد الموارد التكنولوجية فيها حيوية لضمان التشغيل الآمن والفعال للطيران المدني. لكن التطور التكنولوجي طرح تحديات كبرى، بما فيها الهجمات الإلكترونية التي تستهدف أنظمة مراقبة الحركة الجوية والمطارات والمشغلين الجويين. لذلك، تُعد حمايتها من التهديدات الإلكترونية مسألة استراتيجية وحاسمة. ويجب الحفاظ على سلامة وتوافر هذه الأنظمة لتجنب أي انقطاعات قد تؤثر على السلامة التشغيلية واستمرارية النقل الجوي. فالأمن الإلكتروني في هذا السياق لا يقتصر على حماية البيانات والأنظمة فحسب، بل يعزز أيضاً الثقة في البنية الأساسية العالمية للملاحة الجوية.

٣-١ استجابةً لمثل هذه التهديدات، قامت الدول بتنفيذ مجموعة متنوعة من التدابير في مجال الأمن الإلكتروني استناداً إلى القواعد الدولية كتلك التي أعدتها منظمة الطيران المدني الدولي "الإيكاو" والاتحاد الدولي للنقل الجوي "الإياتا" ووكالة السلامة الجوية التابعة للاتحاد الأوروبي (EASA). ومع ذلك، لا تزال هناك ثغرات تحتاج إلى معالجة لضمان حماية شاملة لمنظومة الطيران.

٤-١ أعدت هذه الورقة بما يتوافق مع قرارات الجمعية العمومية ٣٩-١٩، الذي يمثل اعترافاً من المجتمع الدولي بأن الأمن الإلكتروني يمثل أولوية عاجلة بالنسبة للطيران المدني والقرار ٤٠-١٠ المتعلقة باستراتيجية الإيكاو بشأن الأمن الإلكتروني للطيران، مع منهجها التعاوني ومتعدد التخصصات والقرار ٤٠-١٩ الذي يعيد التأكيد على أهمية معالجة الأمن الإلكتروني والمرونة الإلكترونية.

٢- الممارسات الحالية بشأن الأمن الإلكتروني لهيئة أمريكا الوسطى لخدمات الملاحة الجوية (COCESNA)

١-٢ تمت مراعاة أهمية تنفيذ إطار الأمن الإلكتروني للإيكاو في تحديد الوقائع الإلكترونية والحماية منها والكشف عنها والاستجابة لها والتعافي منها. كما يجري التنسيق لمشاركة أفضل الممارسات داخل الإقليم وخارجه مع منظمات دولية مثل الاتحاد الدولي للنقل الجوي "الإياتا" والمنظمة الأوروبية لسلامة الملاحة الجوية "يوروكنترول" ووكالة السلامة الجوية التابعة للاتحاد الأوروبي (EASA).

٢-٢ أما فيما يخص إدارة مخاطر الأمن الإلكتروني، تعمل هيئة أمريكا الوسطى على وضع الأسس لتطبيق منهجيات تحليل المخاطر (ISO 27001 والمعهد الوطني للمعايير والتكنولوجيا (NIST)، و"MITRE ATT&CK"). سيسمح تنفيذ هذه المنهجيات بإجراء تقييمات مستمرة لمواطن ضعف نظام الطيران وإدراج الأمن الإلكتروني في أنظمة خدمات الملاحة الجوية لإقليم أمريكا الوسطى. وبالمثل، تنوي هيئة أمريكا الوسطى إنشاء مركز عمليات أمنية (SOC)، الأمر الذي سوف يمكن المنظمة من تعزيز وضعها الأمني من خلال المراقبة المستمرة والتحليل المتقدم للتهديدات والاستجابة السريعة للوقائع. ومن خلال هذه الخدمة، نسعى إلى تنفيذ نهج استراتيجي وفعال لحماية الأنظمة والبيانات والمستخدمين والتقليل من المخاطر وضمان استمرارية الأعمال والامتثال للوائح التنظيمية.

٣-٢ في مجال التدريب وزيادة الوعي، نقوم حالياً بإعداد برامج تدريب أساسية بشأن الأمن الإلكتروني لجميع موظفي الهيئة، كما سننشأ دورات متخصصة لتدريب الموظفين المعنيين على أفضل الممارسات والاتجاهات الحديثة في الأمن الإلكتروني.

٣- الجوانب الواجب مراعاتها لتحسين الأمن الإلكتروني في مجال الطيران

١-٣ يمكن تعزيز التعاون وتبادل المعلومات مع مزودي خدمات الملاحة الجوية الآخرين من خلال إنشاء منصات آمنة لتبادل المعلومات حول التهديدات ومواطن الضعف في الوقت الفعلي. ويمكن تحقيق ذلك عبر تعزيز التعاون الإقليمي في مجال الأمن الإلكتروني من خلال الاتفاقيات متعددة الأطراف.

٢-٣ يجب تحديد وتنفيذ إطار تنظيمي لتنظيم الأمن الإلكتروني. وينبغي أن يوفر هذا الإطار إرشادات وقواعد واضحة يمكن للمنظمات اتباعها لحماية أصولها الرقمية وضمان سرية البيانات. كما أن تنفيذ إطار تنظيمي قوي يساعد على التقليل من المخاطر ومنع حدوث الوقائع الأمنية وضمان استمرارية العمليات.

٣-٣ ينبغي أن تشمل برامج التدريب على الأمن الإلكتروني الجوانب الفنية والعملية، مثل إدارة الوقائع وتحليل المخاطر وتنفيذ التدابير الوقائية. بالإضافة إلى ذلك، من المهم تعزيز مهارات التواصل والتعاون بحيث يتمكن الموظفون من العمل كفريق ومشاركة المعرفة حول الأمن الإلكتروني. ويعد الاستثمار في التدريب استراتيجية ذات جدوى عالية تعزز من تحصين المنظمة ضد التهديدات الإلكترونية.

٤-٣ يساعد إنكاء وعي الموظفين بالأمن الإلكتروني في التقليل من الأخطاء البشرية التي تُعد سبباً رئيسياً لحدوث الوقائع الأمنية. ووفقاً لدراسات مثل تقرير المخاطر العالمية ٢٠٢٢ الصادر عن المنتدى الاقتصادي العالمي، فإن ٩٥ في المائة من مشكلات الأمن الإلكتروني ناتجة عن الأخطاء البشرية. ويساهم رفع الوعي بشأن التهديدات وأفضل الممارسات في مجال الأمن الإلكتروني في إرساء ثقافة مؤسسية تركز على الأمن الرقمي.

٥-٣ ينبغي أن نعد خطة تحصين إلكتروني تتيح إدراج الأمن الإلكتروني في الخطط الوطنية للسلامة الجوية (NASPs). ولا بد أن تتضمن هذه الخطة استراتيجيات للتعافي من الهجمات الإلكترونية بغية التقليل من آثارها التشغيلية.

٦-٣ يجب أن نقوم بتحديد ومعالجة مواطن الضعف بشكل استباقي من أجل حماية البنية الأساسية للتكنولوجيا وضمان أمن البيانات.

٧-٣ يمكن أن يثمر التعاون مع خبراء الأمن الإلكتروني من مختلف الصناعات مثل التكنولوجيا والمصارف وقطاعات أخرى عن توفير معارف قيمة وموارد متخصصة تعزز حماية أنظمة الطيران.

٨-٣ يوفر اعتماد التكنولوجيات الناشئة مثل الذكاء الاصطناعي والحوسبة السحابية فرصاً لتحسين الكفاءة والسلامة في مجال الطيران المدني. ومع ذلك، من الضروري أن تُنفذ هذه التقنيات مع تدابير أمن إلكتروني قوية لحمايتها من الثغرات

والتهديدات المحتملة. ومن شأن الإدخال الآمن لهذه التقنيات أن يحدث تحولاً في القطاع ولكنه سيتطلب تخطيطاً دقيقاً وإدارة مخاطر مناسبة.

٤- الخلاصة

١-٤ يُعد الأمن الإلكتروني عنصراً أساسياً للسلامة التشغيلية والكفاءة في مجال الطيران المدني. كما تُعد حماية أنظمة الطيران من التهديدات الإلكترونية أمراً ضرورياً لضمان السلامة التشغيلية واستمرارية النقل الجوي. وعلى الرغم من التقدم الكبير في تنفيذ التدابير الوقائية، لا تزال هناك تحديات تستلزم اهتماماً فورياً.

٢-٤ يُعد تعزيز التعاون الدولي وتبادل المعلومات بين المنظمات في قطاع الطيران عبر منصات آمنة والاتفاقيات متعددة الأطراف أمراً حيوياً لتحسين الأمن الإلكتروني، مع إدخال التقنيات المتقدمة واعتماد نهج استباقي لإدارة المخاطر الإلكترونية في مجال الطيران المدني الدولي.

٣-٤ سيوفر تنفيذ القواعد الدولية مثل "ISO/IEC 27001" وإطار عمل "NIST CSF" إرشادات واضحة لحماية الأصول الرقمية وضمان سرية البيانات، مما يساعد على التقليل من المخاطر ومنع حدوث الوقائع.

٤-٤ يسهم تدريب الموظفين وتعزيز الوعي بالأمن الإلكتروني في التقليل من الأخطاء البشرية وتحسين القدرة على الاستجابة للتهديدات وتعزيز تحصين المنظمة.

٥-٤ ومن أجل حماية البنية الأساسية للتكنولوجيا، من الضروري تحديد ومعالجة مواطن الضعف بشكل استباقي من خلال تقييم المخاطر والتحديثات واختبارات الاختراق والرصد المستمر.

٦-٤ يتيح التعاون مع خبراء الأمن الإلكتروني من مختلف الصناعات والتعاقد مع خدمات متخصصة مثل مراكز العمليات الأمنية (SOC) ومزودي خدمات الأمن المُدارة (MSSP) إجراء الرصد المستمر والاستجابة السريعة للوقائع، مما يضمن حماية أفضل لأنظمة الطيران.

٧-٤ يوفر دمج التكنولوجيات مثل الذكاء الاصطناعي والحوسبة السحابية في تدابير قوية للأمن الإلكتروني فرصاً لتحسين السلامة والكفاءة في مجال الطيران المدني، وبذلك ضمان اعتماد هذه التقنيات بشكل آمن وفعال.

— انتهى —