



الجمعية العمومية – الدورة الثانية والأربعون

اللجنة التنفيذية

البند رقم ١٣ من جدول الأعمال: أمن الطيران – السياسة العامة

إنشاء مجموعات إقليمية للأمن الإلكتروني في مجال الطيران في المكاتب الإقليمية لمنظمة الطيران المدني الدولي (الإيكاو)

(ورقة مقدّمة من فنزويلا (جمهورية فنزويلا البوليفارية)

بدعم من ١٦ دولة عضواً في لجنة الطيران المدني لأمريكا اللاتينية)^٢

الموجز التنفيذي

تحوّل قطاع الطيران، بسبب طابعه العابر للحدود الوطنية وما ظل يشهده من عمليات رقمنة متسارعة، إلى صناعة شديدة الترابط، تعتمد على شبكات تكنولوجيا معلومات متنوعة ومعقدة تتطلب تبني تقنيات جديدة ومتطورة لتحسين كفاءة الشبكات والتكيف مع سياق الطيران العالمي الجديد. إلا أنّ هذا الاعتماد على التكنولوجيا يُعرّض قطاع الطيران لمجموعة متزايدة الاتساع من المخاطر الإلكترونية المتطورة والمستمرة، وهي قادرة على تهديد سلامة الطيران وأمنه. وبالتالي، لم يعد الأمن الإلكتروني شاغلاً معزولاً عن الواقع بشكل عام، بل بات تحدياً يتطلب استجابة جماعية ومنسقة تهدف إلى إيجاد حلول تستند إلى القدرات الفردية للدول، مع مراعاة الواقع الإقليمي، لمواجهة تنامي التهديدات الإلكترونية.

الإجراء: الجمعية العمومية مدعوة إلى:

(أ) الإيعاز إلى المجلس بأن يطلب من الأمانة العامة إنشاء وتشكيل مجموعات إقليمية للأمن الإلكتروني في مجال الطيران في أقاليم الإيكاو. وتُعد هذه خطوة استراتيجية لا غنى عنها لحماية سلامة النقل الجوي وأمنه واستمراره، مما يعزز وضعا أكثر قابلية للصمود وأكثر قدرة على الاستباق تجاه التهديدات الإلكترونية، على النحو المنصوص عليه في خطة عمل الإيكاو للأمن الإلكتروني؛

(ب) ضمان أن تتكون هذه المجموعات الإقليمية للأمن الإلكتروني في مجال الطيران من خبراء مهنيين في الأمن الإلكتروني، قادرين على وضع توصيات بشأن التدابير الوقائية وأفضل الممارسات بما يتماشى مع عمل فريق خبراء الأمن الإلكتروني والاحتياجات الإقليمية؛

(ج) الإقرار بأن الأمن الإلكتروني في مجال الطيران يتطلب تخصصاً فنياً محدداً، يختلف عن المجالات الأخرى، والتنسيق مع المجموعات الإقليمية الأخرى لضمان أن يتبنّى كل إقليم، على النحو الملائم، الاستراتيجيات التي وضعها فريق خبراء الأمن الإلكتروني.

^١ قدّمت فنزويلا (جمهورية فنزويلا البوليفارية) هذه الورقة باللغة الإسبانية.

^٢ بلير وبوليفيا (دولة بوليفيا المتعددة القوميات) والبرازيل وكولومبيا وكوبا والجمهورية الدومينيكية وإكوادور والسلفادور وغواتيمالا وهندوراس وجامايكا والمكسيك ونيكاراغوا وبنما وباراغواي وأوروغواي.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي "ضمان السلامة والأمن لكل رحلة جوية"
الآثار المالية:	يُتَرحّ تنفيذ الإجراءات الواردة في هذه الورقة بالاعتماد على الموارد المتاحة في ميزانية البرنامج العادي للفترة الثلاثية الحالية و/أو في المساهمات خارج الميزانية.
المراجع:	الملحق السابع عشر — "أمن الطيران" خطة عمل الإيكاو للأمن الإلكتروني، الفقرات، ١-١-٥، ١-٨-٥، ١-٣-٦، ١-٣-٩، و ١-١١-٥ "استراتيجية الإيكاو للأمن الإلكتروني" (التعاون الدولي)

١- المقدمة

١-١ يتسم الطيران المدني بأنه قطاعٌ شديد الترابط ويقوم على مجموعةٍ من التقنيات. ويعتمد جزءٌ كبيرٌ من البنية الأساسية العالمية للطيران الآن على شبكات تكنولوجيا معلوماتٍ معقدة. ورغم أن هذه التكنولوجيات تُحسّن من كفاءة القطاع، فإنها تُعرّضه في الوقت نفسه لمجموعةٍ واسعةٍ ومتزايدةٍ من التهديدات الإلكترونية المعقدة والمتطورة باستمرار، وهي قادرة على اختلاس معلومات حساسة، وإحداث اضطراب في العمليات، وفي نظم الملاحة الجوية والاتصالات والاستطلاع، ذات الأهمية الحاسمة، وإلحاق أضرار جسيمة بسمعة الطيران والثقة في سلامته، على سبيل المثال لا الحصر.

٢-١ ولذلك، فإنّ من الضروري تصميم آليات وقنواتٍ فعّالةٍ لتخفيف المخاطر الإلكترونية أو تقليلها إلى الحد الأدنى في هذا القطاع، نظراً لطبيعته العابرة للحدود الوطنية، مما يعني أن أي هجوم إلكتروني في دولةٍ واحدةٍ قد تُسفر عن آثارٍ أو تداعياتٍ تمتد إلى إقليمٍ بأكمله أو عبر العالم. وبالتالي، لم يعد الأمن الإلكتروني شاغلاً معزولاً يقتصر على أمن الطيران، بل أصبح تحدياً يتطلب استجابةً جماعيةً ومنسقةً تتجاوز الحدود الوطنية وتراعي واقع كل إقليم وخصائصه.

٣-١ للتهديدات الإلكترونية سماتٌ خاصة تُميّزها عن التهديدات التقليدية التي تواجه سلامة وأمن الطيران: فهي تتطور بوتيرةٍ أسرع بكثير، كما يتضح من الظهور السريع لنواقل الهجمات والثغرات الأمنية الجديدة، التي يمكن أن تنشأ وتُنفذ في أي مكان في العالم؛ ويصعب على وجه العموم تحديد هوية المهاجمين وسماتهم، إذ قد يكونون مجهولي الهوية في بعض الأحيان. ويختلف ذلك عن التهديدات أو المخاطر الأخرى، التي تتطلب في العادة وجوداً مادياً أو اقتراباً من الهدف، ولذلك فإن التهديدات الإلكترونية تُحدث تغييراً جذرياً في أساليب الكشف عنها والتصدي لها والتحقيق فيها.

٤-١ وتشجّع منظمة الطيران المدني الدولي (الإيكاو) الجهود التعاونية، من خلال مناقشات الأمن الإلكتروني داخل المجموعات الإقليمية أو المبادرات المماثلة في المجال الأمني. ومع ذلك، فيما يتعلق بالأمن الإلكتروني، من المهم اتباع نهج أفقي ومشترك بين القطاعات، ودمجه في مختلف تخصصات الطيران. وغالباً ما تتطوي مناقشات الأمن الإلكتروني على تفاصيل تقنية معقدة تتطلب فهماً شاملاً للبنية الأساسية لتكنولوجيا المعلومات وعمليات الطيران.

٥-١ ويعني كل ذلك ضرورة الاعتراف بأن الأمن الإلكتروني في مجال الطيران قد وصل إلى مستوى من التعقيد والخطورة يتطلب معالجةً واهتماماً من ذوي التخصص، في منتدىٍ يضمّ مهنيين لهم خلفيات فنية محددة، وتنسيق عملهم مع مجموعات أو مبادرات مماثلة في مجال أمن الطيران، وغيرها من المجموعات الإقليمية، حيث تُناقش المسائل المتعلقة بالأمن الإلكتروني في مجال الطيران.

٢- التحليل

١-٢ ستعمل مجموعات الخبراء الإقليمية المقترحة بشكل أساسي على مضاعفة العمل الذي يقوم به فريق خبراء الأمن الإلكتروني التابع للإيكاو، حيث تُترجم الاستراتيجية العالمية إلى إجراءات عملية على المستوى الإقليمي، مما يضمن أخذ الأمن الإلكتروني للطيران - وهو مسألة متشعبة ومتعددة التخصصات - على محمل الجد في كل إقليم والتعامل معه على النحو الملائم والواقعي. ولتحقيق هذه الغاية، من الضروري الإقرار بالعمل الجاد الذي أنجزه خبراء الفريق والبناء عليه، فقد بذل هذا الفريق جهوداً جبارة في إعداد الأدلة والإرشادات وأفضل الممارسات المناسبة لبيئة الطيران المعقدة.

٢-٢ وغالباً لا تكون الدول على علمٍ بنطاق وتطبيق عمل فريق خبراء الأمن الإلكتروني أو أنها تستفيد منه استفادةً محدودة. ومن هذا المنطلق، ستكون مجموعات الأمن الإلكتروني في مجال الطيران في أقاليم الإيكاو بمثابة قنوات حيوية لنشر المبادئ التوجيهية العالمية وتكييفها وتنفيذها في كل سياقٍ من السياقات الإقليمية. وبالتالي، يمكن للدول أن تستفيد استفادةً مباشرةً من خبرة الفريق والموارد التي يوفرها، مما يُسرّع من نضج وضع الأمن الإلكتروني في مجال الطيران في كل إقليم.

٣-٢ ويُعد إنشاء مجموعات الأمن الإلكتروني في مجال الطيران في أقاليم الإيكاو بصورة رسمية من الحاجات الملحة. وستسترشد هذه المجموعات بهيكل فريق الخبراء وتنظيمه وأهدافه، وستتبع نموذجاً للتعاون يعزّز المرونة الجماعية، ولا يقتصر على تعزيز تبادل المعلومات والتدريب المتخصص فحسب، بل يُسهّل أيضاً اتخاذ الإجراءات المنسقة والمرنة. وسيضمن ذلك نهجاً أكثر تركيزاً وفعالية، يقوم على حماية البنية الأساسية لتكنولوجيا المعلومات وعمليات الطيران، وبالتالي يحافظ على سلامة الطيران واستمراريته في أقاليمنا.

— انتهى —