A41-WP/158
EX/72
2/8/22

منظمة الطيران المدني الدولي

ورقة عمل

الجمعية العمومية – الدورة الحادية والأربعون

اللجنة التنفيذية

البند رقم ١٤: أمن الطيران — السياسة العامة

تقديم التدريب على بناء القدرات والأمن الإلكتروني للدول

(مقدمة من غيانا وتؤيدها الأرجنتين وبوليفيا والبرازيل وكولومبيا والجمهورية الدومينيكية والإكوادور والسلفادور وغواتيمالا وبنما وبيرو وأروغواي وفنزويلا)

الموجز التنفيذي

الأمن الإلكتروني هو ظاهرة متعددة التخصصات تشكل تهديداً للطيران المدني. وقد اعترفت الإيكاو بهذا التهديد لأمن الطيران المدني الدولي وردّت على ذلك بوضع استراتيجية الأمن الإلكتروني وخطة عمل الأمن الإلكتروني. وبالرغم من أن هذه السياسات العامة والإرشادات مفيدة للدول، من الضروري أن تكون الدول مزودة بالمعرفة والقدرات والتدريبات والموارد ذات الصلة من أجل التخفيف على نحو فاعل من الهجمات والمخاطر الإلكترونية على الصعيد الوطني والإقليمي والدولي. وبالتالي تطلب ورقة العمل هذه من الإيكاو تخصيص موارد لبناء قدرات الدول من أجل تحقيق أهداف الركائز السبعة لاستراتيجية الأمن الإلكتوني التي حددت تبعاً لذلك:

أ) التعاون الدولي؛
ب) التنظيم الإداري؛
ج) التشريعات واللوائح الفعالة؛
د) السياسة العامة للأمن الإلكتروني؛
هـ) تبادل المعرفة؛
و) التخطيط لإدارة الحوادث وحالات الطوارئ؛
ز) بناء القدرات والتدريب وثقافة الأمن الإلكتروني.

الإجراء: الجمعية العمومية مدعوة إلى:

أ) توجيه المجلس للطلب من الأمانة العامة تخصيص موارد للصمود بوجه الأمن الإلكتروني ولبناء قدرات الدول الصغيرة. ومن بين المجالات المتعلقة بالاحتياجات التدريب على الوعي بالأمن الإلكتروني، والتدريب على إدارة حوادث الأمن الإلكتروني والاستجابة لحالات الطوارئ، وتدريب المدربين على الأمن الإلكتروني، وبرنامج التدريب على منح التراخيص؛

ب) والطلب إلى الإيكاو تعزيز وإنشاء آلية للتعاون لتعزيز برامج الإرشاد والتبادل الفني في مجال الطيران بين الدول.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالأهداف الاستراتيجية للأمن والتسهيلات.
المراجع:	الملحق ١٧ — أمن الطيران استراتيجية الأمن الإلكتروني للطيران خطة عمل الأمن الإلكتروني

١- المقدمة

١-١ يُتوقع أن تزداد الحركة الجوية للطيران المدني ويزداد معها اعتمادها على التكنولوجيا. وتؤدي زيادة الاعتماد على التكنولوجيا إلى زيادة التهديدات والمخاطر بحيث يصبح الأمن الإلكتروني مسألة هامة للدول وإلى الحاجة إلى بناء القدرة على الصمود بوجه التهديد الذي تمثله هذه المخاطر. والأمن الإلكتروني في الطيران أمر لا مفر منه، لأنه يطرح على نطاق واسع يشمل جوانب السلامة والأمن والملاحة الجوية ونظم تكنولوجيا المعلومات والاتصالات وعمليات الطيران العامة. وتوفر استراتيجية الإيكاو للأمن الإلكتروني وخطة عمل الإيكاو للأمن الإلكتروني الإرشادات الضرورية للدول للبدء بإرساء الأساس لبنية أساسية متينة للأمن الإلكتروني. غير أن ذلك يحتاج إلى بناء القدرات والتدريب وإلى ثقافة الأمن الإلكتروني والتعاون بين الوكالات والتعاون الأقاليمي.

١-٢ ولبناء بينة أساسية متينة، يتعين على الدول اتباع الركائز السبعة لاستراتيجية الإيكاو للأمن الإلكتروني في الطيران واعتماد خطة عمل الإيكاو للأمن الإلكتروني التي ترسي الأساس لتعاون الدول وأصحاب المصلحة في الصناعة من أجل تطوير القدرة على تحديد الهجمات الإلكترونية على الطيران المدني ومنعها وكشفها والتعافي من أثرها، فضلاً عن استحداث إطار للتعاون. وتقترح خطة عمل الأمن الإلكتروني عدة تدابير وإجراءات ينبغي أن تعتمدها الدول لتحقيق أهداف الركائز السبعة. تشمل هذه الأهداف التعاون الدولي بين الدول، ووضع هياكل التنظيم الإداري، وصياغة تشريعات وأطر تنظيمية وطنية فعالة، ووضع سياسات عامة للأمن الإلكتروني، وتبادل المعلومات ذات الصلة بين الدول، والتخطيط لإدارة الحوادث وحالات الطوارئ وبناء القدرات، والتدريب وتعزيز ثقافة الأمن الإلكتروني لبناء القدرة على الصمود من أجل معالجة هذه الظاهرة العالمية.

١-٣ يعتبر بناء القدرات أساسياً لإنشاء بنية أساسية (عالمية) متينة للأمن الإلكتروني. وهو الأساس الذي تقوم عليه إمكانية تحقيق الركائز السبعة. وتُشجّع الإيكاو على تعزيز بناء القدرات الضرورية وتوفيرها للدول وبخاصة الدول الصغيرة.

٢- المناقشة

٢-١ اتخذت غيانا عدة مبادرات لمكافحة الهجمات الإلكترونية وبناء القدرة على الصمود في الأمن الإلكتروني، وهو ما يتواءم مع الركائز السبعة لاستراتيجية الأمن الإلكتروني في الطيران. وتتولى رئاسة هذه المهمة الهيئة الوطنية لإدارة البيانات التي تعتبر الكيان المحدد لرصد وحماية البيانات داخل غيانا. وقد باشرت هذه الهيئة بصياغة السياسات العامة الوطنية للأمن الإلكتروني والقواعد القياسية والتشريعات واللوائح التي نشرت من اجل التشاور بشأنها عبر لجان مشتركة بين الوكالات. وهذه عملية تكرارية تحتاج إلى مساهمات من الوكالات المعنية، ولا سيما تلك التي لها بنية أساسية حيوية. وبالنظر إلى القيود والتحديات المفروضة على الدول الصغيرة، ثمة حاجة إلى تقديم إرشادات وتدريبات خارجية بشأن كيفية معالجة الأمن الإلكتروني بشكل كلي. وبالرغم من أن تبادل المعلومات يتم على الصعيد الوطني بين الوكالات وأن التدريب يطلب عبر لجنة مشتركة بين الوكالات، فإن بناء القدرات كدولة هو أمر ضروري.

٢-٢ يستتبع بناء القدرات تقديم تدريب ذي صلة للعاملين في الطيران من أجل زيادة معارفهم وكفاءاتهم ومهاراتهم وقدراتهم في الأمن الإلكتروني. ويتطلب أيضاً توفير موارد بشرية ورأسمالية ذات صلة لإنشاء بنية أساسية متينة للأمن الإلكتروني. ويمكن بناء هذه القدرات عن طريق تنفيذ ورش عمل وطنية وإقليمية ودولية. ويتطلب ذلك توفير تدريب كاف لتعزيز قدرات الدول على التخطيط لإدارة حوادث الأمن الإلكتروني والاستجابة لحالات الطوارئ. وهذ أمر لا مفر منه لأنه ينجم عن عدم القدرة على إيقاف الهجمات الإلكترونية بمجموعها بالرغم من إمكانية تخفيفها بواسطة نظم متينة. لذلك، وبالرغم من حدوث هجمات إلكترونية، من المهم أن تكون الدول قادرة على بناء القدرة على الصمود من أجل استمرار الأعمال التجارية.

٣-٢ يعتبر توفير دورات التدريب وورش العمل وبرامج التمرّس بالمهنة وبرامج التوجيه وما إلى ذلك ضرورياً لبناء القدرات في الدول الصغيرة. ويمكن تقديم هذه الدورات إلى كل دولة على حدة وإلى المنطقة كلها، حسبما يقتضيه الحال.

٣- الاستنتاج

٣-١ تعترف ورقة العمل هذه بحاجة الدول إلى بناء القدرات وتعزيز القدرة على الصمود في الأمن الإلكتروني.

– انتهى –