A40-WP/295
TE/119
1/8/19

**منظمة الطيران المدني الدولي**

**ورقة عمل**

# الجمعية العمومية – الدورة الأربعون

## اللجنة الفنية

**البند رقم ٣٠ من جدول الأعمال: المسائل الأخرى المعروضة على نظر اللجنة الفنية**

## تطبيق ضوابط الأمن الإلكتروني للدول في مجال الطيران

(مقدمة من نيوزيلندا)


**الموجز التنفيذي**

تتناول ورقة العمل هذه وضع أطر الإيكاو للأمن الإلكتروني في مجال الطيران في سياق الضوابط الحالية للأمن الإلكتروني التي لا تتعلق بقطاعات محددة وتستخدمها الدول. وتقترح هذه الورقة أن تركّز الإيكاو جهودها على وضع مبادئ متماسكة ومتفق عليها تمكّن الدول من معالجة المسائل المرتبطة بالأمن الإلكتروني.

**الإجراءات:** تُدعى الجمعية العمومية إلى القيام بما يلي:

أ) أن تأخذ علماً بأن تنفيذ قواعد قياسية عالمية متسقة وذات طابع إلزامي مُفرط في مجال الأمن الإلكتروني قد يتعارض مع الأطر الوطنية للدول في مجال الأمن الإلكتروني ويحدّ من قدرة الدول على الامتثال للقواعد والتوصيات الدولية الصادرة عن الإيكاو؛

ب) أن تشجّع الإيكاو على التركيز على إعداد إرشادات تستند إلى المبادئ بشأن الأمن الإلكتروني في قطاع الطيران لمساعدة الدول على إدراج الطيران في الأطر الوطنية مع مراعاة القواعد القياسية المقرّرة لأمن المعلومات مثل معيار أيزو ISO 27000؛

ج) أن تشجّع الإيكاو على تقديم الإرشادات بشأن الغرض من إطار الثقة وتطبيقه.


| | |
|---|---|
| الأهداف الاستراتيجية: | ترتبط ورقة العمل هذه بالهدفين الاستراتيجيين: الأمن والتسهيلات، والسلامة. |
| الآثار المالية: | لا توجد. |
| المراجع: | ورقة العمل (AN-Conf/13-WP/270) بعنوان "مفهوم منظومة النُظم للأمن الإلكتروني في الطيران (٢٠١٨/٩/٢٨) |

## ١ – المقدمة

١–١ في ظلّ التقدّم المستمر في المجال التكنولوجي وزيادة مستويات تشعّب نظم الطيران، أصبحت سلامة وأمن نظام الطيران العالمي تتوقّفان بشكل متزايد على الضوابط الفعالة للأمن الإلكتروني.

١–٢ وأصبحت الحاجة إلى وضع الضوابط الفعالة للأمن الإلكتروني أمراً معمولاً به في مجموعة واسعة من قطاعات شتى ولا يقتصر هذا الأمر على مجال الطيران على الإطلاق. وبدون الأمن الإلكتروني الفعال، ستجد المؤسسات المعنية صعوبة في تقديم منتجات وخدمات رقمية كي يتسنى لها الحفاظ على ثقة زبائنها والجهات المعنية.

١–٣ ولابد للدول أن تضطلع بدور في ضمان وجود مؤسسات وقطاعات هامة على المستوى الوطني لمواصلة تحقيق مستويات عالية من الأمن الإلكتروني. وسيختلف النهج المتّبع باختلاف الدول وفقا للتهديدات والقدرات ومصالح الأمن القومي.

١–٤ وبالرغم من أن نوع الضوابط الأمنية التي تضعها مختلف المؤسسات سيتم تكييفها بشكل عام مع ما لديها من احتياجات وقدرات والقطاع الذي تعمل فيه، فإن مصالح الأمن القومي ستفرض متطلبات شاملة. وستبقى المصلحة الوطنية دائما تحظى بالأولوية على مصلحة قطاع أو مؤسسة بعينها.

١–٥ ويعتمد الطيران العالمي اعتماداً كبيراً على الإرسال الرقمي للمعلومات بما يتسم بالسلامة والأمن بين أعضاء أوساط الطيران، لاسيما فيما بين الدول. وقد عرضت ورقة العمل رقم (AN-Conf/13-WP/270) المقدّمة خلال المؤتمر الثالث عشر للملاحة الجوية مفهوم نهج "منظومة النظم" في مجال الأمن الإلكتروني. ويُـقرّ هذا النهج بأن نظام الطيران ككل يتكون من عدد من النظم الفرعية التي تديرها مجموعة من الجهات المعنية وأنه لابد لهذه الجهات أن تنظر فيها بشكل شامل لتهيئة بيئة عمل تتسم بالأمن.

١–٦ وقد تم وضع إطار الثقة لدى الإيكاو بما يمكّن من إقامة روابط اتصال موثوقة بين الجهات المعنية. ويشمل هذا الإطار المبادئ التالية:

١–٦–١ يتم ضمان قابلية التشغيل البيني بين جميع الجهات المعنية وفقا لإطار ثقة مشترك وهيكل من أجل تقديم خدمات الرسائل التي تتسم بالسلاسة والفعالية على المستوى العالمي.

١–٦–٢ ويتم تعزيز مرونة الاتصالات إلى الحد الأقصى من خلال استخدام مفاهيم التصميم التي تحدّ من سطح التهديدات. ويتضمن ذلك تقسيم الشبكة والتطبيقات، بالإضافة إلى تحديد أشكال الحماية في البنى التحتية وتقليص عدد النظم المشاركة.

١–٦–٣ تعزيز إجراءات تحديد الهوية والمصادقة والترخيص والنزاهة والسرية.

١–٧ وبالرغم من أن مفهوم إطار الثقة ينطوي على قيمة، إلاّ أن هناك عدم وضوح يكتنِف الغرض منه وإمكانية تطبيقه. كما سيتطلب وضع هذا الإطار إيلاء مزيد من الاهتمام لمصالح الأمن القومي للدول بما يضمن تحديد الأدوار التي يضطلع بها بوضوح.

## ٢ – المناقشة

٢–١ تفرض المصالح الوطنية للدول قيوداً على طبيعة أطر الأمن الإلكتروني التي يمكن أن تنفّذها مختلف القطاعات والمنظمات. وعندما توجد متطلبات تنظيمية وقواعد قياسية وطنية تتعلق بأمن المعلومات، فإنها ستحظى بالأولوية على القواعد القياسية الخاصة بقطاع أو مؤسسة بعينها.

٢-٢ وبناءً عليه، من المحتمل الحدّ من قدرة الدولة على الامتثال للقواعد والتوصيات الدولية الإلزامية الصادرة عن الإيكاو بالنسبة للأمن الإلكتروني في مجال الطيران بسبب ما لديها من أطر في مجال الأمن الوطني. وسيختلف حجم هذه القيود باختلاف الدول وحجم الطابع الإلزامي للقواعد والتوصيات الدولية نفسها.

٢-٣ وبالمثل، فمن غير المرجح أن يُسهم اتباع نهج إلزامي وموحّد للغاية في التنظيم الفعال لمجال تشهد فيه التكنولوجيا وبيئة التهديدات تطوراً سريعاً. أما الشروط العالمية التي تتسم بطابع إلزامي مُفرط فقد تعوق قدرة الدولة على مواكبة التغييرات، وقد لا تناسب هذه المتطلبات بنفس القدر أنواع مختلفة من العمليات.

٢-٤ وبالرغم من تباين احتياجات خدمات الأمن الإلكتروني لمختلف الدول والمشاكل المتعلقة بفرض شروط دولية جد إلزامية، لابد من وضع مجموعة متسقة ومتفق عليها من المبادئ تحكم النقل الآمن للمعلومات بين الجهات المعنية.

٢-٥ ولدعم تنفيذ هذه المبادئ، ينبغي وضع المواد الإرشادية للإيكاو مع التركيز على مساعدة الدول على دعم الأمن الإلكتروني في مجال الطيران كجزء لا يتجزأ من الأطر الوطنية. ولتحقيق ذلك، من المرجح أن يتمثل الحلّ الأكثر فعالية في اتباع نهج يقوم على الأداء أو على المبادئ.

٢-٦ ومن خلال اعتماد نهج يقوم على المبادئ، يمكن لمختلف الدول أن تعمل على تكييف إرشادات الإيكاو بما يمكن من تنفيذ إطار ثقة عالمي وفقا للمتطلبات الوطنية. أما القواعد القياسية الحالية المرتبطة بأمن المعلومات على أساس المبادئ، مثل معيار أيزو ISO 27000 فتوفر أساساً لهذه الإرشادات. وهناك أربعة مجالات تركيز يمكن معالجتها بشكل أمثل هي:

٢-٦-١ **النُظم الإدارية:** تعزيز الأمن الإلكتروني على مستوى القيادة العليا من أجل حماية أهم الأصول الرقمية للمنظمة. وتضطلع المجالس والمديرون التنفيذيون في نهاية المطاف بالمسؤولية عن نتائج أي شكل من أشكال الحوادث الإلكترونية، بما في ذلك التأثير على ثقة الجهات المعنية والزبائن.

٢-٦-٢ **الاستثمار:** الاستثمار في مجال الأمن الإلكتروني للحدّ من المخاطر وزيادة الإيرادات. ويعتبر الاتفاق على مستوى النظم الإدارية بشأن رغبة المنظمة في مواجهة المخاطر وتحديد الأصول الرئيسية من الخطوات الأولى الحاسمة للتأكد من توجيه الاستثمار وتحقيق توازنه بشكل مناسب.

٢-٦-٣ **الاستعداد:** إعداد المؤسسة المعنية لاكتشاف أي شكل من أشكال الحوادث المرتبطة بالأمن الإلكتروني ومواجهتها والتعافي منها. ويتعلق الأمر هنا بمسألة "متى" وليس "ما إذا" كانت ستتعرض المؤسسة المعنية لحادث من الحوادث المرتبطة بالأمن الإلكتروني. كما أن الاستعداد للحوادث يمكّن المؤسسات من خفض حدّة مجموع المخاطر المرتبطة بالأمن الإلكتروني من خلال التعافي منه بشكل فوري وبفعالية.

٢-٦-٤ **سلسلة الإمدادات:** الحرص على مراقبة المخاطر المرتبطة بالأمن الإلكتروني والتوعية بها في سلسلة الإمدادات للمنظمة المعنية. وينطوي هذا المجال على أهمية خاصة في قطاع الطيران نظراً لأنه دائما ما يتطلب توفير المعدّات والخدمات سلاسل إمدادات طويلة. ويشمل ذلك المكوّن الفني لتصميم النُظم والجانب المتعلق بالعامل البشري لتصميم العمليات.

٢-٧ أما الإرشادات المصاغة بشكل جيّد والقائمة على الأداء، وفقاً للقواعد القياسية المحددة في مجال أمن المعلومات، فستشكل عنصراً هاماً لمختلف المؤسسات في قطاع الطيران وستشجع على اتباع نهج متسق يشمل العناصر الحاسمة للضوابط الفعالة في مجال الأمن الإلكتروني.

٢-٨ ولدى وضع هذه الإرشادات ينبغي أيضاً مراعاة الحالات التي يتعين فيها تحديد بعض الضوابط الدنيا وكيفية تناولها مع مراعاة الأُطر التي تطبقها مختلف الدول.

٢-٩ ويتيح وضع إطار الثقة لدى الإيكاو فرصة لتحديد البروتوكولات اللازمة لتبادل المعلومات بين الجهات المعنية، وإن كان لابدّ من زيادة توضيح الغرض منها وتطبيقها.

٢-١٠ وينبغي النظر في وضع إطار الثقة بالاقتران مع أطر الأمن الإلكتروني التي تنفذها الجهات المعنية. أما جودة أمن تبادل البيانات فتتوقّف فقط على جودة أمن مصادر البيانات وهو ما يعتمد على فعالية الضوابط التي تعتمدها المؤسسات والدول.

**– انتهى –**