منظمة الطيران المدني الدولي

ورقة عمل

A41-WP/74
EX/36
26/7/22

الجمعية العمومية — الدورة الحادية والأربعون

اللجنة التنفيذية

البند رقم ١٤: أمن الطيران — السياسة العامة

إنشاء إطار عام للأمن الإلكتروني

(مقدمة من تشيكيا بالنيابة عن الاتحاد الأوروبي والدول الأعضاء فيه[١] والدول الأعضاء الأخرى في اللجنة الأوروبية للطيران المدني[٢] والدول الأعضاء في اللجنة الأفريقية للطيران المدني[٣] ويوروكنترول)

الموجز التنفيذي

تزداد أهمية الأمن الإلكتروني بشكل مستمر بما أن التكنولوجيات الجديدة واعتماد الطيران بشكل أكبر على تكنولوجيا المعلومات والنظم التشغيلية الرقمية يولد مواطنِ ضعف جديدة، بالإضافة إلى فرص جديدة. ومع زيادة فهم المجال الإلكتروني يتبين أنه محفوفٍ بعدد من الصعوبات المحددة، مما يبرز الحاجة إلى من التطور وإحراز تقدم نحوٍ نهج محدد للتخفيف من المخاطر. ونظرا إلى أهمية الأمن الإلكتروني المتزايدة، على الدول والإيكاو مضاعفة جهودها دعما لوضع إطار عام للأمن الإلكتروني، بالإضافة إلى إرساء ثقافة الأمن الإلكتروني والتدريب عليها.

الإجراء: الجمعية العمومية مدعوة إلى القيام بما يلي:

أ) أن تطلب من الإيكاو النظر في الخطوات التي يجب اتخاذها من أجل إحراز تقدم نحو إعداد المواد الإرشادية بشأن تقييم مخاطر الأمن الإلكتروني في مجال الطيران، مع مراعاة الفاعلين المعنيين والحاجة إلى منظور شامل متعدد التخصصات والعوامل المحددة الواردة في ورقة العمل هذه؛

ب) أن تطلب من الإيكاو الانتهاء من تجميع القواعد والتوصيات الدولية القائمة ذات الصلة بهذا الموضوع والقواعد القانونية الدولية الأخرى التي يمكن للدول والمنظمات الاعتماد عليها من أجل إدراج المخاطر الإلكترونية ضمن أطر الطيران الخاصة بها؛

---

[١] النمسا وبلجيكا وبلغاريا وكرواتيا وقبرص وتشيكيا والدانمرك وإستونيا وفنلندا وفرنسا وألمانيا واليونان وهنغاريا وأيرلندا وإيطاليا ولاتفيا وليتوانيا ولكسمبورغ ومالطا وهولندا وبولندا والبرتغال ورومانيا وسلوفاكيا وسلوفينيا وإسبانيا والسويد.

[٢] ألبانيا وأرمينيا وأذربيجان والبوسنة الهرسك وجورجيا وآيسلندا ومولدوفا وموناكو ومونتينيغرو ومقدونيا الشمالية والنرويج وسان مارينو وصربيا وسويسرا وتركيا وأوكرانيا والمملكة المتحدة.

[٣] الجزائر وأنغولا وبنن وبوتسوانا وبوركينا فاسو وبوروندي والكاميرون والرأس الأخضر وجمهورية أفريقيا الوسطى وتشاد وجزر القمر والكونغو وكوت ديفوار وجمهورية الكونغو الديمقراطية وجيبوتي ومصر وغينيا الاستوائية وإريتريا وإسواتيني وإثيوبيا وغابون وغامبيا وغانا وغينيا وغينيا-بيساو وكينيا وليسوتو وليبيريا وليبيا ومدغشقر ومالاوي ومالي وموريتانيا وموريشيوس والمغرب وموزامبيق وناميبيا والنيجر ونيجيريا ورواندا وساو تومي وبرنسيبي والسنغال وسيشيل وسيراليون والصومال وجنوب أفريقيا وجنوب السودان والسودان وتوغو وتونس وأوغندا وجمهورية تنزانيا المتحدة وزامبيا وزمبابواي.

ج) أن تطلب من الإيكاو والدول المتعاقدة لديها تكثيف الجهود من أجل تعزيز ثقافة منفصلة مكرسة للأمن الإلكتروني وتنظيم الأنشطة اللازمة من أجل دعم تطوير الموارد والقدرات البشرية الكافية بهدف إدارة الأمن الإلكتروني وتحصين الشبكة الإلكترونية في مجال الطيران المدني؛ د) أن تطلب من الإيكاو النظر في تنظيم تمارين في مجال الأمن الإلكتروني على المستويين العالمي والإقليمي.	
الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي "الأمن والتسهيلات".
الآثار المالية:	
المراجع:	

١- المقدمة

١-١ اعتمدت الجمعية العمومية للإيكاو في دورتها الأربعين القرار ٤٠-١٠ "معالجة الأمن الإلكتروني في مجال الطيران الدولي". ويعالج القرار الأمن الإلكتروني من خلال نهج عملي شامل متعدد التخصصات، مع إعادة التأكيد على أهمية والطابع الملح لحماية نظم البنى الأساسية الهامة للطيران المدني وبياناتها من الهجمات الإلكترونية، ويناشد الدول بتنفيذ استراتيجية الإيكاو للأمن الإلكتروني في مجال أمن الطيران (أكتوبر ٢٠١٩). وتنفّذ الاستراتيجية من خلال خطة عمل الأمن الإلكتروني وبدعم من فريق خبراء الأمن الإلكتروني الحديث المنشأ، والذي سيستفيد من عمل مجموعة دراسة الأمن الإلكتروني التابعة للأمانة العامة.

١-٢ وبما أن الرقمنة تؤثر تأثيراً بالغاً على الاقتصادات وتعيد رسم ملامح قطاع الطيران، يصبح الأمن الإلكتروني حالياً أهم من أي وقت مضى. ولا يزال الأمن الإلكتروني يشكل تحدياً لكافة القطاعات في فترة التعافي من جائحة فيروس كورونا. كما تستخدم المؤسسات طرق عمل أكثر افتراضية قد تعرضها للتهديدات الإلكترونية بشكل أكبر، مما يقتضي مضاعفة الجهود من أجل إعداد إطار عام للأمن الإلكتروني مع أخذ هذه المواصفات بعين الاعتبار.

٢- عناصر محددة في المشهد العام للأمن الإلكتروني من أجل وضع نهج لإدارة المخاطر

٢-١ يعرض مجال الأمن الإلكتروني صورة فريدة عن التهديدات. فعليه أن لا يركز فقط على الجماعات الإرهابية التي تسعى إلى شن هجمات مباشرة والتسبب في خسائر جسيمة، إنما يجب أن يأخذ في الحسبان مجموعة الدوافع والجهات الفاعلة الأخرى المحتملة، والتي قد تشمل هيئات منظمة كبرى وناشطين وقراصنة إلكترونيين مجرمين، يسعون، على سبيل المثال، إلى التسبب في تعطيل أو أنشطة قسرية أو استعراض القوة أو لفت انتباه وسائل الإعلام أو تحقيق مكاسب مالية. كما أن الهجمات قد تؤثر عن قصد أو عن غير قصد على الطيران المدني، مما قد يهدد السلامة ويؤثر على القطاع سواء بشكل مباشر أو غير مباشر.

٢-٢ ويجب مراعاة عناصر أخرى في إدارة المخاطر الإلكترونية، منها العدد الكبير لمقدمي الخدمات غير الخاصة بالطيران المتعاملين مع منظومة الطيران والذين قد يكون لديهم مفهوم مختلف عن مخاطر الأمن الإلكتروني وضروراته.

٢-٣ كذلك يتسم المجال الإلكتروني بوجود لوائح الدول التي قد يكون معمولا بها في كافة القطاعات، بدون وجود عنصر محدَّد للطيران.

٢-٤ ويشير ما ورد أعلاه إلى ضرورة وضع نهج محدَّد لتقييم مخاطر الأمن الإلكتروني حيث:

أ) الخبرات المطلوبة، لا سيما فيما يتعلق بمواطن الضعف وتدابير التخفيف، لابد وأن تجمع بين الخبرة والمعرفة في مجالي الطيران وتكنولوجيا المعلومات؛

ب) يجب أن يكون نطاق التقييم محدداً بشكل واضح وأن يركز على السلامة والأمن والقدرة على التصدي للأزمات وذلك بالنسبة للوظائف الحيوية المشتركة في ما بين الهيئات/المشغلين الفرادى ومختلف المجالات؛

ج) يمكن لتقييم المخاطر أن يحدد أسباب التعطل المحتملة والتي تفتقر إلى بديل لها، وذلك من منظور (عالمي) لأمن المعلومات من أجل معالجتها بشكل ملائم.

٣- إنشاء إطار عام للأمن الإلكتروني يأخذ الخصوصيات بعين الاعتبار

٣-١ عند إنشاء إطار عام للأمن الإلكتروني، على قطاع الطيران أن يعد نهج لا تكتفي فقط بتجاوز الحدود التقليدية في مجالات الطيران (على غرار الحاجة إلى منظور كلي (مثلاً إدارة الحركة الجوية) ومنظور فردي للطيران)، وإنما يأخذ أيضاً بعين الاعتبار المواقع المختلفة للقطاعات غير ذات الصلة بالطيران واللوائح الوطنية الأفقية (غير الخاصة بالطيران) على النحو الوارد في الفقرتين ٢-٢ و٢-٣ أعلاه. ومن الضروري ضمان الاتساق وتفادي الازدواجية والفجوات وعبء الرقابة واللوائح التنظيمية الواقع على عاتق الدول والمشغلين بلا داعٍ عند تنفيذ إطار عام للأمن الإلكتروني.

٣-٢ ويعتبر قطاع الطيران مؤهلاً للاستفادة من الإجراءات والمسؤوليات والأدوار في مجال الطيران الدولي بل والإضافة إليها. وتعد القواعد والتوصيات الدولية التي أصدرتها الإيكاو في مجال سلامة وأمن الطيران أساساً متيناً يمكن الاعتماد عليه على مستوى الحكومات وعلى المستوى التنظيمي. وينطبق الأمر نفسه على آليات الإبلاغ وتبادل المعلومات. كما توجد مواثيق قانون الجو الدولي لتجريم الأفعال التي تهدد السلامة والتي يجب استخدامها قدر الإمكان.

٣-٣ وفي هذا السياق، يحبذ أن تقوم الدول والمنظمات بمراجعة وثائق الإيكاو عن الأمن الإلكتروني والنظر فيها، وتنفيذ القواعد والتوصيات الدولية ذات الصلة بالأمن الإلكتروني. ومن المهم أيضاً بالنسبة إلى الدول والمنظمات أن تعيد النظر في سلامة وأمن الطيران، بالإضافة إلى نظم القانون الجنائي في مجال الطيران من منظور رقمي حرصاً على أن تبقى الأدوار والمسؤوليات حديثة ومنسقة بشكل ملائم.

٤- أهمية العنصر البشري في الأمن الإلكتروني

٤-١ يعتبر العنصر البشري في صميم الأمن الإلكتروني، كما أقرت الإيكاو بذلك في استراتيجيتها للأمن الإلكتروني في مجال الطيران (٢٠١٩).

٤-٢ ومع زيادة الرقمنة المتزايدة والترابط الإلكتروني في منظومة الطيران، تشتد الحاجة إلى مضاعفة الجهود من أجل الاستجابة للطلب المتنامي على التوعية والتدريب والمناهج الأكاديمية المحدثة والموظفين المدرَّبين بشكل ملائم الذين يتمتعون بالخبرات المتقاطعة المتشعبة في مجال الطيران والأمن الإلكتروني، ودعماً لكل تلك النواحي.

٤-٣ وأطلقت الأمانة العامة للإيكاو أول دورة تدريبية للإيكاو عن الأمن الإلكتروني وتحصين الشبكة الإلكترونية بعنوان "أسس قيادة الأمن الإلكتروني والإدارة الفنية في مجال الطيران"، بالإضافة إلى دورة أخرى عن "إدارة المخاطر الأمنية في إدارة الحركة الجوية" التي أُعدت بالشراكة مع يوروكنترول. ومن المهم الاستفادة من هذه الجهود المستحبة والدروس المستفادة.

٤-٤ وكما ورد في استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران، تعتبر التدريبات على الأمن الإلكتروني أداة مفيدة من أجل اختبار تحصين الشبكة الإلكترونية وتحديد التحسينات التي يجب إدخالها وبالتالي التشجيع وبقوة على القيام بذلك. بالإضافة إلى التدريبات على مستوى فرادى الدول الأوروبية، تتمتع أوروبا بخبرة إقليمية في هذا المجال لتسخّرها لمصلحة أسرة الطيران الدولية[٤]. ويرجى من الإيكاو دراسة إمكانية استضافة مثل هذه التدريبات.

٤-٥ وكما أُشير في عام ثقافة الأمن الذي أطلقته الإيكاو، من الضروري توسيع نطاق مفهوم ثقافة الأمن والسلامة بما يتجاوز حدود الواقع الملموس. ويحبذ أن تبادر الدول والمنظمات إلى الاستفادة من إنجازات عام ثقافة الأمن من خلال تعزيز ثقافة الأمن الإلكتروني وتبادل أفضل الممارسات. وعلى الإيكاو تعزيز الجهود لهذه الغاية، بما في ذلك إعداد المواد الإرشادية الملائمة.

— انتهى —

[٤] *يستهدف تمرين "الأمن الإلكتروني في أوروبا لعام ٢٠١٨* (Cyber Europe 2018) *الذي نظّمته وكالة الاتحاد الأوروبي لأمن الشبكة والمعلومات مهنيين ومنظمات معنية بأنشطة أمن المعلومات في قطاع الطيران؛ كما نظّمت الخلية الأوروبية للتنسيق في مجال أزمات الطيران* (EACCC) *تمرينا لإدارة الأزمات في عام ٢٠١٨ نتيجة لهجمة إلكترونية على برنامج إلكتروني للمراقبة وتعد تمرينا لإدارة الأزمات في عام ٢٠٢٢ مع محاكاة حالة قصور واسع النطاق لبنى تحتية لشبكة رقمية أوروبية نتيجة لهجمة إلكترونية؛ ونظمت وكالة السلامة الجوية التابعة للاتحاد الأوروبي* (EASA) *تمارين في مجال الأمن الإلكتروني.*