A39-WP/175
EX/64
9/8/16

منظمة الطيران المدني الدولي

ورقة عمل

الجمعية العمومية – الدورة التاسعة والثلاثون

اللجنة التنفيذية

البند رقم ١٦: أمن الطيران — السياسة العامة

الأمن الإلكتروني للطيران المدني: التدابير التي يمكن أن يتخذها واضعو التنظيمات وأصحاب المصلحة

(مقدمة من الأرجنتين وبلجيكا وفرنسا وغينيا وجمهورية لاو الديموقراطية الشعبية وناميبيا وناورو ونيبال وهولندا ونيجيريا وجمهورية مولدوفا والاتحاد الروسي وسانت لوشيا والمملكة العربية السعودية والسنغال وسيراليون وسنغافورة وجنوب أفريقيا وسويسرا وجمهورية مقدونيا اليوغسلافية السابقة وترينيداد وتوباغو والإمارات العربية المتحدة والمملكة المتحدة)

الموجز التنفيذي

تشكل التهديدات الإلكترونية للطيران المدني شاغلا كبيرا بالنسبة لجميع أصحاب المصلحة على الصعيد العالمي. لذلك، لزاماً على الإيكاو وسلطات أمن الطيران وقطاع صناعة الطيران وأصحاب المصلحة الآخرين في مجال الطيران المدني أن يتعاونوا للرفع من مستوى الوعي بهذه التهديدات وإعداد سياسات ونهج وتدابير عملية ومستدامة، بما في ذلك اعتماد تدابير للتدريب وبناء القدرات، وذلك لحماية الطيران المدني من الهجمات الإلكترونية والحد من آثارها. ونظراً لتداخل الأجزاء المتعددة المكونة مجمل لنظام العالمي للطيران المدني، من الضروري توثيق عرى التعاون لمعالجة هذه التحديات.

الإجراء: الجمعية العمومية مدعوة إلى:

أ) أن تأخذ علما بفحوى هذه الورقة، لاسيما التدابير التي يمكن أن يتخذها كل من واضعي التنظيمات وأصحاب المصلحة لمعالجة التهديدات الإلكترونية التي تحدق بعمليات الطيران المدني؛

ب) أن تحث الإيكاو على إعداد إطار عالمي للأمن الإلكتروني لأصحاب المصلحة في الطيران المدني؛

ج) أن تحدد هيئة ضمن الإيكاو للعمل على إعداد هذا الإطار العالمي وللتنسيق مع الهيئات المعنية الأخرى في الإيكاو وأصحاب المصلحة الآخرين.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالأهدف الاستراتيجية (أ)– السلامة؛ و(ب) سعة وكفاءة الملاحة الجوية؛ و(ج) الأمن والتسهيلات
الآثار المالية:	ما من آثار مالية إضافية
المراجع:	ورقة العمل A39-WP/14، استراتيجية الإيكاو الشاملة لأمن الطيران (ICASS) ورقة العمل A39-WP/15، إعداد خطة عالمية لأمن الطيران (GASeP) ورقة العمل A39-WP/16، البيان الموحّد بسياسات الإيكاو المستمرّة المتعلقة بأمن الطيران ورقة العمل A39-WP/17، معالجة الأمن الإلكتروني في الطيران المدني AVSECP/27 Restricted (Yellow Cover) Report (*English only*)

١- المقدمة

١-١ تم الإقرار بأن التهديدات الالكترونية لنظم الطيران المدني شأنه شأن نظم القطاعات الأخرى تمثل شاغلا كبيرا. فالسبل عديدة ومتعددة للإرهابيين والأشخاص ذوي النوايا الخبيثة لإطلاق الهجمات الإلكترونية ضد أصحاب المصلحة ومقدمي خدمات الطيران المدني والبنية الأساسية التابعة لهم. فيمكنهم أن يشلوا عمليات الطيران المدني، بما في ذلك الاختراق غير القانوني لنظم ملاحة الطيران ومراقبة الطائرات والتدخل بنظم الرادار والاتصالات وإفساد نظم متعددة في المطارات. على الرغم من أن هذه الهجمات ضد قطاع الطيران اعتبر مستواها، لغاية اليوم، منخفضاً من حيث الآثار، فإن أي اعتداء إلكتروني ضد عمليات الطيران المدني يمكن أن يأتي بشبه كارثة، إذ يلحق الخسائر الكبيرة ويخل بخدمات الطيران المدني و/أو يتسبب بأضرار في البنية الأساسية الحرجة. وتتفاقم هذه الشواغل مع زيادة اعتماد شركات الطيران والمطارات ومقدمي خدمات الملاحة الجوية وغيرها من الجهات المعنية، (مثل شركات الخدمات الأرضية ومقدمي الخدمات الأمنية وشركات الوقود ووكلاء الشحن وغيرها) على تكنولوجيا المعلومات والاتصالات لتنفيذ عملياتها.

٢- الجهود للتصدي للتهديدات الإلكترونية

٢-١ في السنوات الأخيرة، أمست الجهات المعنية بالطيران المدني تولي مزيداً من الأهمية للتهديدات الإلكترونية. وفي عام ٢٠١٤، قامت الإيكاو والاتحاد الجوي للنقل الجوية (الإياتا)، والمجلس الدولي للمطارات ومنظمة خدمات الملاحة الجوية المدنية والمجلس التنسيقي الدولي لاتحادات صناعات الطيران والفضاء بوضع خطة عمل مشتركة لمعالجة هذه التحديات. كما أعدت الإياتا مجموعة من الأدوات المساهمة في توفير الأمن الإلكتروني والخاصة بشركات الطيران، في حين أن العديد من المطارات ومقدمي خدمات الملاحة الجوية ومصنعي الطائرات قد اتخذوا تدابير عديدة لتحصين أمن العمليات ضد التهديدات الإلكترونية.

٢-٢ وعلى الصعيد الدولي، عالج واضعو تنظيمات أمن الطيران المدني هذه المسائل على مستوى فريق خبراء الإيكاو لأمن الطيران (AVSECP). وقد قدم فريق عمل التهديدات والمخاطر سلسلة من عمليات التقييم والمشورة إلى الفريق المعني بمخاطر التهديدات الإلكترونية، وبدأ التنسيق فيما بين هذا الفريق وأفرقة الإيكاو الأخرى المعنية بالسلامة من أجل ترشيد الجهود في معالجة هذا الموضوع المشترك.

٢-٣ على الرغم من هذه التدابير، ما زال العديد من أصحاب المصلحة يتخبطون في خضم هذه التحديات. وإن إزكاء الوعي والترويج للحوار بين أصحاب المصلحة بشأن التهديدات الإلكترونية من الطرق المفيدة للمساعدة في زيادة الفهم لهذه المخاطر. ومن شأن التقييم المفصل للمخاطر أن يسمح لأصحاب المصلحة بالكشف عن الثغرات الأمنية بحيث يتخذوا الخطوات اللازمة لسدها. وفي يوليو ٢٠١٥، نظمت سنغافورة مؤتمراً بشأن الأمن الإلكتروني بالتشارك مع الإيكاو والإياتا وبدعم من العديد من الدول وأصحاب المصلحة في قطاع صناعة الطيران، وقد توافد إلى هذا المؤتمر العديد من الخبراء الآتين من قطاعات مختلفة في الطيران المدني لمناقشة هذه المواضيع. وشملت طائفة المشاركين مشغلي المطارات وشركات الطيران ومصنعي محركات الطائرات وجهات المناولة الأرضية ومقدمي خدمات الأمن ومقدمي التجهيزات الأمنية والمنظمات الدولية المعنية بالطيران المدني وواضعي التنظيمات. ومن بين المواضيع الرئيسية التي نوقشت نذكر ما يلي:

أ) التهديدات والمخاطر التي تترتب عن الهجمات الإلكترونية المحدقة بنظام العالمي للطيران المدني: أن التقييم المنتظم الذي يقوم به فريق WGTR لهذه المخاطر والتهديدات، يمكن أن يستخدمه كل من الإيكاو والجهات المعنية لإعداد تدابير وقائية وتدابير التصدي الفعالة؛

ب) الاعتبارات المتعلقة باعتماد التدابير الوقائية، وإجراءات التصدي، فضلا عن اجراءات الطوارئ وتدابير الإنعاش بعد التهديدات في حالة وقوع هجوم إلكتروني على عمليات الطيران المدني؛

ج) التدابير التي يمكن أن يتخذها بعض أصحاب المصالح للتصدي للتهديدات الإلكترونية؛

د) المخاطر المحدقة على وجه الخصوص بقطاع الطيران المدني تعزى إلى كون الهجمات الإلكترونية من شأنها أن تنجح أكثر في قطاع تكون فيه عناصره مترابطة إلى حد بعيد، وإلى كون آليات الدفاع والتصدي الإلكترونية لدى الطيران المدني لم تصل بعد إلى مستوى مؤات لمعالجة هذه التهديدات التي تتعاظم بصورة سريعة؛

هـ) الحاجة إلى اعتماد نهج أفقي يشمل قطاع الطيران برمته لضمان التنفيذ المتسق والمتناسب والفعال.

٣- الإجراءات التي يمكن أن يتخذها واضعو التنظيمات وأصحاب المصلحة

٣-١ تم الكشف عن عدد من الإجراءات التي يمكن أن يتخذها كل من واضعي التنظيمات وأصحاب المصلحة وهي تتضمن ما يلي:

أ) التكليف، على وجه السرعة، الجهات المسؤولة عن هذا الموضوع، ابتداءً من **المستوى العالمي** حيث يمكن أن يكون مفيدا **للإيكاو أن تنشئ إطارا عالمياً لأصحاب المصلحة في مجال الطيران المدني من أجل معالجة التهديدات الإلكترونية.** ويمكن لهذا الإطار، الذي ينبغي أن يستند إلى أفضل الممارسات الحالية في مجال أمن المعلومات ويطور على أساس الاستشارة الوثيقة بين الخبراء في مجال أمن الطيران وسلامة الطيران، أن يتضمن مجموعة من المبادئ والإرشادات والنُهج الموجهة إلى عناية واضعي التنظيمات وقطاع الصناعة؛

ب) على **مستوى الدولة، من الضروري لسلطات أمن الطيران (بالتنسيق مع السلطات الأخرى المسؤولة عن الأمن الإلكتروني على المستوى الوطني) أن تقوم بإعداد وتوفير المراقبة التنظيمية لمعالجة التهديدات الإلكترونية.** وينبغي لنظام المراقبة التنظيمية أن يشمل مجمل قطاع الطيران المدني وجميع المعنيين في هذا النظام من وجهة نظر شاملة بسبب تداخل تلك الجهات فيما بينها؛

ج) **على مستوى صاحب المصلحة بصورة فردية، ينبغي لكل صاحب مصلحة أن ينشئ مجموعة خاصة به من التدابير لحماية عملياته من التهديدات الإلكترونية، لاسيما تلك النظم الهامة المرتبطة بسلامة الطيران وأمنه؛**

د) ينبغي لأصحاب المصلحة أن يتصدوا للتهديدات الإلكترونية بأسرع وقت ممكن. لذلك، من الضروري لقطاع الطيران المدني **أن يعد التدابير للكشف المبكر والتنسيق والمعالجة السريعة.** فإن الإبلاغ بالوقائع الخاصة بأمن الطيران إلى أفرقة التصدي في حالات الطوارئ لأجهزة الكمبيوتر (CERTs) أو لمراكز تبادل المعلومات وتحليلها سيمكن من إطلاق التحذير المبكر إلى أصحاب المصلحة الآخرين، وينبغي أن يشجع هذا الابلاغ على الصعيد الوطني إلى جانب التنسيق الدولي بريادة الإيكاو؛

هـ) ولما كان الأمن الإلكتروني يتطور بدافع التهديدات والاتجاهات الجديدة في مجال التكنولوجيا، **ينبغي الجمع بين العناصر المكونة من مجموعات الأشخاص والعمليات والتكنولوجيا والنظم المختلفة لضمان توفير القدرة على تحديد المخاطر والتخفيف من حدتها.**

و) **من الضروري تبادل المعلومات وأفضل الممارسات بين وكالات الأمن الإلكتروني للطيران المدني.** سيساعد ذلك الدول وأصحاب المصلحة في الكشف بصورة مشتركة وجماعية عن الاتجاهات وتحديد التهديدات واعتماد التدابير المضادة الفعالة. ومن الضروري لوكالات الاستخبارات والوكالات الأخرى أن تواصل بذل جهودها لتحسين فهمها للتهديدات الإلكترونية المحدقة بالطيران المدني؛

ز) نظرا للطبيعة المتداخلة لنظم معلومات الطيران المدني، **من الضروري تحقيق الفهم المشترك لكل البيانات والنظم الحيوية والضرورية لسلامة نظام الطيران المدني وأمنه واستمراريته.** وينبغي لواضعي التنظيمات في مجال الطيران أن يعملوا بصورة مشتركة لتحديد معايير النظم الحاسمة (على الصعيد العالمي والإقليمي و/أو الوطني)، وذلك بهدف الاسترشاد بتلك المعايير أثناء التنفيذ؛

ح) **من الضروري تدريب موظفي الطيران المدني عبر مختلف اقسام منظومة الطيران المدني لكي يكونوا مدركين للمخاطر والتهديدات التي تترتب عن الهجمات الإلكترونية ويتصدوا لها على نحو سريع ومناسب.** وإن الكشف عن الثغرات ورفع حالة التأهب بصورة مبكرة ازاء أي تطورات أو نشاطات مشتبه بها، من شأنه أن يجنب أو يحتوي أي هجوم إلكتروني أو يساعد في التقليص والحد من الأعطال التي يمكن أن تعرقل العمليات. ومن المهم ايضاً إدراج تحديات الأمن الإلكتروني في برامج التدريب على أمن الطيران، فضلا عن توظيف المتخصصين والمدققين في مجال أمن الطيران الذين يألفون موضوع الأمن الإلكتروني.

ط) **من الضروري توسيع نطاق ثقافة أمن الطيران حتى تشمل تقييماً أفضل لتهديدات الأمن الإلكتروني.** فإذا اقتنع كبار الإداريين بضرورة التصدي لهذه التهديدات ووفروا الدعم المتين لتدريب الموظفين واستثمروا في الموارد لمعالجة هذه التهديدات، سيتمكن قطاع الطيران المدني من التصدي على نحو يتسم بقدر أكبر من الكفاءة.

–انتهى–