A39-WP/187[1]
EX/72
10/8/16

منظمة الطيران المدني الدولي

ورقة عمل

الجمعية العمومية - الدورة التاسعة والثلاثون

اللجنة التنفيذية

بند جدول الأعمال ١٦: أمن الطيران - السياسة

الاستراتيجية الدفاعية للأمن السيبراني

(مقدمة من منظمة خدمات الملاحة الجوية المدنية (كانزو))

الموجز التنفيذي

الأمن السيبراني هو واحد من أهم القضايا ذات الصلة والموضوعات الأكثر إثارة للجدل في مجال الطيران المدني. إن تطور أنظمة الطيران يجابهها المزيد من المخاطر الجديدة، والتي تؤثر وتستمر بسبب تزايد الاعتماد على تكنولوجيا المعلومات. ليس فقط منظومات إدارة حركة الطيران (ATM) ولكن أيضاً منظومات الطائرات، ومنظومات إدارة المطارات، ومنظومات الحجز ومعلومات الطيران ومعلومات الطقس يمكن أن تتأثر بنفس القدر من الحوادث السيبرانية، والتي لا ترتبط فقط بالسرية، ولكن بالأساس بمدى التوافر والاستمرارية.

الإجراء: تنعقد الجمعية العمومية من أجل الموافقة على التوصية الواردة في الفقرة ٥

الأهداف الاستراتيجية:	ورقة العمل هذه ترتبط بالهدف الإستراتيجي (ج) - *الأمن والتسهيلات*.
الآثار المالية:	تخفيض تكاليف التأمين؛ التخفيف من التهديدات والمخاطر في ضوء المرونة والسلامة والتقليل من التكاليف المتعلقة بإدارة الأزمة وآثارها الاجتماعية.
المراجع:	الملحق ١٧ لاتفاقية شيكاغو - *الأمن*؛ الوثيقة Doc. 8973؛ الوثيقة Doc. 9985؛ الوثيقة Doc. 9954؛ مرشد تقييم مخاطر الأمن السيبراني لمنظمة خدمات الملاحة الجوية المدنية

١ - مقدمة

١-١ ولا يزال الطيران المدني هدفاً محتملاً على مستوى عال للمجرمين والإرهابيين. إن الالتزام بحماية الطيران المدني ضد أفعال التدخل غير المشروع توجب التعامل مع التهديدات المتطورة، بما في ذلك تلك التي لها طابع تكنولوجي. إن المجتمع يتوقع دائما صفر حوادث وأحداث غير متوقعة بسبب الخروقات الأمنية لصناعة الطيران بصفة عامة. هذا المنظور سوف يضع ثقة العملاء النهائيين في مجال النقل الجوي. تعتبر شبكة النقل الجوي أمرا ضروريا للاقتصاد العالمي وأساسا للتجارة

[1] توفّر منظمة خدمات الملاحة الجوية المدنية هذه الورقة باللغات العربية والإنجليزية والصينية والفرنسية والروسية والإسبانية

الدولية والسياحة والاستثمار والازدهار. يمكن لأي تعطل لكفاءتها أن يؤدي إلى اضطراب اقتصادي واجتماعي لا يستهان به في جميع أنحاء العالم. إن تطوير المنظومات المعقدة، القابلة بطبيعتها للتشغيل المتبادل، في بيئة عالمية ودولية، تتطلب أسلوبا منهجيا لإدارة الأمن للتمكن من الرصد المستمر للموارد، والتكامل العملياتي بين تكنولوجيا المعلومات (IT)، والأمن المنطقي والمادي. هذا ما ينبغي القيام به من خلال تقييم مستمر لمستوى التهديد والضعف المحتمل، بهدف المنع والرد والاستجابة لأفعال التدخل غير المشروع. وهذا يتطلب أيضاً التنسيق الوثيق بين جميع الجهات الفاعلة في منظومة الطيران، والدول والجهات المعنية ذات الصلة. لا يكفي مجرد الامتثال للوائح، في حين أنه من الضروري دائماً إظهار العناية الواجبة في حماية الأرواح البشرية في الأجواء وعلى الأرض وضمان الأمن والاستمرارية والمرونة وانتظام المنظومة. مجموعة العمل بالتهديد والمخاطر (TRWG) لمنظمة الطيران المدني الدولي قد شددت أيضاً على أن نظام الطيران العالمي داخل منظومته المعقدة من المعلومات والاتصالات، وهي بالتأكيد هدفاً محتملاً للهجمات السيبرانية الخطيرة. إن هدف قابلية التشغيل المتداخل وفتح الشبكات في مقابل مفهوم التشغيل المركزي للشبكة يمكن من اقتسام الوقت الحقيقي من المعلومات والبيانات التشغيلية ويفتح المنظومة للمزيد من الثغرات.

١-٢ وقد أثارت بالفعل منظمة الطيران المدني الدولي القلق بشأن الأمن الإلكتروني والذي يمكن أن يكون عائقا في تنفيذ خطة الملاحة الجوية العالمية (GANP) وقد دعمت مبادرة مشتركة مع أصحاب المصالح الكبرى في الطيران، من أجل إجراء تقييم منتظم للأطر السيبرانية القائمة (سايبر مجموعة صناعية عالية المستوى [IHLG] والموقعة في ٢٠١٤/١٢/٥ بمونتريال).

١-٣ أثناء الاجتماع النقاشي لفريق خبراء أمن الطيران لمنظمة الطيران المدني الدولي (AVSECP/27) المنعقد في مارس ٢٠١٦ قام عدد كبير من الدول الأعضاء بتسليط الضوء على ضرورة الارتقاء بالممارسة الحالية الموصى بها في الملحق ١٧ (الأمن) بشأن الأمن السيبراني؛ إلى مستوى قياسي. ومع ذلك، تمسك غالبية الأعضاء بالرأي القائل بأن الأمن السيبراني لا يقتصر على منظومة أمن الطيران وحدها. وأكد الأعضاء إلى الحاجة الماسة لضمان التنسيق المناسب، بما في ذلك التوافق مع الملاحق الأخرى، وهي ملحق ٣، ٦، ١٠، ١١، ١٤ و١٥. وعلاوة على ذلك، فإنه بالتنسيق مع جلسات النقاش الأخرى ذات الصلة، من الضروري قبل رفع مستوى الممارسات الموصى بها داخل المعايير القياسية، فإن هناك حاجة واضحة للتشاور مع لجنة الملاحة الجوية لمنظمة الطيران المدني الدولي (ANC).

١-٤ تريد منظمة خدمات الملاحة الجوية المدنية (كانزو) أن تؤكد على أهمية حماية جميع المعلومات والنظم الرقمية في إطار منظومة الطيران. وهذا أمر حيوي لضمان حماية وسلامة الجمهور، الركاب، الطاقم، موظفي الخدمات الأرضية، ومرافق الطيران والطائرات ضد أفعال التدخل غير المشروع التي يتم ارتكابها سواء على الأرض أو في الجو. ويمكن أن تطلب إجراءات محددة لتعزيز هذا المفهوم في الدول الأقل نمواً، بوصفها تقع في إطار مبادرة منظمة الطيران المدني الدولي وفقاً لمبدأ "عدم ترك أي بلد وراء الركب".

٢- الحاجة إلى التوضيح في مجال الأمن السيبراني

٢-١ تلاحظ منظمة خدمات الملاحة الجوية المدنية (كانزو) أن هناك درجة معينة من الارتباط بشأن مصطلح "الأمن السيبراني"، وهو المستخدم للتعبير عن التهديد الذي يشكله الخصوم، فضلاً عن الحاجة إلى تقييم وتحديد نقاط الضعف في أنظمة تكنولوجيا المعلومات. وعلاوة على ذلك فهو يستخدم لوصف كيفية تنفيذ خطط الطوارئ الفعالة بشكل مرن.

٢-٢ وتؤكد منظمة خدمات الملاحة الجوية المدنية (كانزو) بأن الإستراتيجية الأمنية السليمة للطيران المدني ينبغي أن ينظر إليها ليس فقط على المستوى التكنولوجي للاستحقاق، ولكن على أساس النهج الوقائي المنهجي للوصول إلى الهدف الرئيسي لأمن الطيران. وهذا لا يمكن أن يتحقق إلا بإتباع منهج يتناول القاعدة أولاً في اتجاه القمة، بما في ذلك كامل المنظمة، مع أخذ العوامل البشرية في الاعتبار.

٢-٣ وقد تم الإعلان عن هذا الهدف بشكل واضح داخل مفهوم *تشغيل إدارة الحركة الجوية العالمية* (وثيقة الإيكاو Doc 9854) والذي وصف دور الأمن بأنه أمر ضروري وعرضه بطريقة مبتكرة للغاية:

"تشير كلمة الأمن إلى الحماية ضد التهديدات التي تنبع من الأفعال المتعمدة (الإرهاب على سبيل المثال) أو أفعال غير مقصودة (الخطأ البشري أو الكوارث الطبيعية على سبيل المثال) والتي تؤثر على الطائرات أو الأشخاص أو المنشآت على الأرض. الأمن الكافي هو التوقع الرئيسي لمجتمع إدارة حركة الطيران. ولذلك ينبغي على منظومة ماكينة الصراف الآلي أن تسهم في الأمن، وأن يتم حماية منظومة ماكينة الصراف الآلي والمعلومات ذات الصلة بماكينة الصراف الآلي ضد التهديدات الأمنية".

٢-٤ من هذا المنظور – ارتباط المعايير الرئيسة بأمن تكنولوجيا المعلومات – فإن هدف توفير الإتاحة، النزاهة والسرية يشير إلى الالتزام العام للدول المتعاقدة في ضمان حماية المقومات الأساسية للطيران المدني، عملاً باتفاقية شيكاغو وخاصة فيما يتعلق بملحق منظمة الطيران المدني الدولي رقم ١٧ (الأمن).

٣- منهج جديد

٣-١ تسلط منظمة خدمات الملاحة الجوية المدنية (كانزو) الضوء على الأصول الضرورية لسلامة الطيران المدني قد تختلف فيما بين الجهات المعنية للطيران على أساس أهدافها؛ مثل الحكومات ومقدمي خدمات الملاحة الجوية، شركات الطيران، والمطارات، الشركات المصنعة، والقوات المسلحة، وما إلى ذلك، ومن الممكن تحديد بعض موضوعات الأمن السيبراني الخاصة بالطيران، والشائعة لجميع أفراد المجتمع، والمحددة باحتياجات خاصة:

أ) لضمان عدم الوصول إلى المعلومات الهامة إلا لمن أذن له، من أجل منع أعمال التدخل غير المشروع عن طريق التهديدات الداخلية، على الخدمة المركزية للمشغل بشكل مستقل

ب) للوفاء بالالتزام، على أساس الحس السليم وحسن *النية*، لتحديد ومعالجة نقاط الضعف في النظم الحيوية، حتى تتماثل مع الاجتهاد والتعقل العاديين.

ج) لتمديد إدارة المخاطر، نحو المخاطر الناجمة عن تزايد الاعتماد على موارد تكنولوجيا المعلومات الذي يملكها مشغل واحد.

د) أن يكون هناك إدارة استجابة للتعامل مع الحادث وإدارة الأزمات بشكل مناسب، بما في ذلك التخطيط للطوارئ.

هـ) لتقييم الآثار الناجمة عن انتهاكات الأمن (السيبراني) ليس فقط على مشغل واحد ولكن على الصناعة بصفة عامة، في إطار برنامج أمن للطيران المدني الوطني.

٣-٢ من ناحية أخرى، الأمن السيبراني لا يختلف عن أسلوب أمن الطيران التقليدي، وإنما هو مجرد امتداد طبيعي للمبادئ الأساسية الواردة في الملحق ١٧ (الأمن)، والمواد الإرشادية، ومعالجة التهديدات ونقاط الضعف الأكثر شيوعاً والتي تشير إلى الأمن المادي.

٣-٣ من المرجح إن التهديد السيبراني على الطيران واحد من القضايا الأمنية الرئيسة في أي برامج تحديث جديدة، مثل برنامج السماء الأوربية الواحدة (SES)، إبحاث برنامج السماء الأوربية لإدارة حركة الطيران (SESAR)، الجيل التالي (NEXTGEN) وغيرها التي يتم تطويرها على المستوى الإقليمي. ويبدو أنها أحد أكثر المشغلات ذات العلاقة بأجزاء أخرى في صناعة الطيران. وكمورد حاسم، يجب أن يتم التعامل مع المعلومات كأي أصول أساسية أخرى ينبغي حمايتها والعمل على نجاح منظومات إدارة حركة الطيران. كل هذه البرامج، لا تقتصر على إدارة حركة الطيران ولكن تشمل أيضاً مشغلات الطائرات، المطارات، القوات المسلحة وغيرها، والتي تستند على مفهوم إدارة المعلومات على نطاق واسع للنظام (SWIM)، تسهيل التبادل التشغيلي للمعلومات والخدمات عبر النظام بأكمله. إن مفهوم إدارة المعلومات على نطاق واسع (SWIM) سيحسن من عملية صنع القرار التعاوني، ويوفر أفضل نوعية معلومات مطلوبة على أساس الحاجة إلى معرفة الوقت المناسب

وللمستلم الصحيح. إن إدارة المعلومات على نطاق واسع (SWIM) هي المساعد الرئيسي لبيئة تكنولوجيا المستقبل لقطاع الطيران حيث ينبغي النظر للبنية التحتية المرتبطة بها كبنية تحتية هامة حيث يعتبر الأمن بمثابة الشرط الأساسي عند التصميم.

٣-٤ في هذا الصدد، حيث لا يزال يلتزم الأمن العام نحو الدول المتعاقدة بالآثار المترتبة على السيادة الوطنية والدفاع والمخابرات، ومطبقي القانون، فإن هناك حاجة إلى النظر في خصوصية بيئة الطيران من حيث اتخاذ إجراءات أكثر فعالية.

٣-٤-١ إن المبادرات المتعلقة بالموضوع ما زالت في طريقها إلى التنفيذ أو قد تم تنفيذها بالفعل. وفيما يلي بعض النتائج الأخيرة: ينص موقف الاتحاد الأوروبي بوضوح بخصوص الإنترنت داخل إدارة حركة الطيران والصادر بلائحة المفوضية الأوروبية (المسجلة برقم 1035/2011) على وجود علاقة واضحة بين نقاط الضعف الأمنية والمتطلبات الملزمة المنصوص عليها بخصوص الأمن السيبراني. إن إدارة الطيران الاتحادية في الولايات المتحدة (FAA) خلال عرضها الذي عرضته على مجلس الشيوخ الأمريكي قد أعلنت عن الهدف المناسب للأمن السيبراني (القسم ٤١٠٩) والذي وضع كهدف صعب، يشتمل على مجموعة واسعة من الإجراءات للتعامل مع مسائل الإنترنت. وقد ركزت أيضاً الدول الأخرى جهدها الرقابي بنفس الطريقة على الأمن السيبراني للطيران.

٣-٤-٢ نظراً لأهمية الأمن السيبراني بالنسبة للطيران المدني، فإن منظمة خدمات الملاحة الجوية المدنية (كانزو) تؤيد تماماً أي مبادرة تهدف إلى تحقيق الاندماج الكامل لموضوع الأمن السيبراني في إطار برامج وطنية وإقليمية لأمن الطيران وتعلن إمكانية مشاركتها بنشاط.

٤- الختام

٤-١ الأمن السيبراني في مجال الطيران هو موضوع ينبغي معالجته بطريقة منهجية وواقعية، نظراً إلى تداعياته وآثاره على الصناعة برمتها وعلى ثقة الجماهير عامة.

٤-٢ تشجع منظمة خدمات الملاحة الجوية المدنية (كانزو) على مبادرة دولية متجددة تحت قيادة منظمة الطيران المدني الدولي وبطريقة فعالة ومستدامة وفقاً لمبدأ " لا نترك بلد خلفنا".

٤-٣ بادرت مجموعات صناعية رفيعة المستوى، في أعقاب خطة عمل عن الأمن السيبراني في شهر ديسمبر من عام ٢٠١٤، بوضع إطار عمل لتعزيز التعاون الطوعي في هذا المجال. وينبغي استكمال البرنامج ودعمه بالتأييد المنتظم والنظر أكثر عمقاً نحو هذا المجال المتشعب في مجال الطيران المدني والمعبر عنه بالأمن السيبراني.

٥- التوصيات

٥-١ دعت الجمعية العمومية إلى تكليف الأمانة العامة لمنظمة الطيران المدني الدولي بمسألة ملحة تتعلق بجعل الأمن السيبراني جزءا فعليا لأمن الطيران بطريقة مستدامة وفعالة. كما تنعقد الجمعية العمومية من أجل الموافقة على التوصية التالية:

أن تقوم الجمعية العمومية بالآتي:

أ) النظر في مضمون الورقة وتأييدها، الاعتراف بأهميتها وتأثيرها المحتمل على الطيران المدني؛

ب) الموافقة على أن تضع منظمة الطيران المدني الدولي إستراتيجية جديدة للأمن السيبراني في مجال الطيران كمجال متنامي داخل الموضوعات المتعلقة بأمن الطيران، بهدف مواءمة المبادرات الحالية على المستويين الإقليمي والوطني؛

ج) توصي الدول الأعضاء بتركيز الاهتمام على نقاط الضعف في المنظومات والشبكات بدلاً من التركيز على التهديدات والنظر في الآثار المترتبة على صناعة الطيران المدني بأكملها؛

د) كما توصي بتعيين منتدى لشركات الطيران وذلك لتبادل أفضل الممارسات داخل بيئة آمنة/ موثوقة بحيث تكون هناك مشاركة للأدوات والتقنيات الفعالة والتي تعزز من الأمن ضمن التكنولوجيا الحالية والمستقبلية؛

هـ) توصي الدول الأعضاء باستعراض المبادرات الأخيرة التي تم تقديمها خلال (AVSECP/27) من أجل رفعه إلى مستوى معيار للممارسات الحالية الموصى بها ٤-٩-١ و ٤-٩-٢ من الملحق ١٧؛

و) الإحاطة علما بدليل كانزو *"مرشد الأمن السيبراني وتقييم المخاطر"*[٢].

-انتهى-

[٢] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide