AN-Conf/14-WP/124[1]
29/6/24

منظمة الطيران المدني الدولي

ورقة عمل

المؤتمر الرابع عشر للملاحة الجوية

مونتريال، كندا، من ٢٦/٨/ إلى ٦/٩/٢٠٢٤

البند ٤ من جدول الأعمال: الترابط الفائق في شبكة الملاحة الجوية
٤-٢: الأمن الإلكتروني وقدرة نظام المعلومات على الصمود

المبادئ التوجيهية التنظيمية للأمن الإلكتروني لخدمات الحركة الجوية

(مقدّمة من الأرجنتين وتشارك في رعايتها ١٩ دولة عضواً في لجنة الطيران المدني لأمريكا اللاتينية)[2]

الموجز التنفيذي

تعرض ورقة العمل هذه الاعتبارات المتعلقة بتحقيق الاتساق في الأحكام التنظيمية لخدمات الحركة الجوية، لغرض إدراج المواصفات والأساليب والإجراءات المتعلقة بسيناريوهات الهجمات المحتملة للبرمجيات الخبيثة ضد خدمات الحركة الجوية، من أجل ضمان الرصد المستمر لما يتلقاه الموظفون من تدريب أولي وتدريب لتجديد معارفهم.

الإجراءات: يُرجى من المؤتمر القيام بما يلي:

أ) دعم المبادرات المعروضة في ورقة العمل هذه، مع طلب إجراء تحليل لفائدة إدراج لوائح وأساليب الأمن الإلكتروني الخاصة بخدمات الحركة الجوية في إطار الطيران العالمي؛

ب) تشجيع الدول على دمج استراتيجياتها الوطنية للأمن الإلكتروني مع استراتيجيات الإيكاو بشأن الطيران المدني من أجل إقامة ثقافة أمن إلكتروني في مجال خدمات الحركة الجوية وإدراج السياسات والاستراتيجيات والآليات بوصفها ضمانات، من خلال وضع الأحكام التنظيمية المقترحة.

[1] قدمت الأرجنتين هذه الورقة باللغة الإسبانية.

[2] أروبا (مملكة هولندا) وبليز وشيلي وكولومبيا وكوستاريكا وكوبا والجمهورية الدومينيكية وإكوادور والسلفادور وغواتيمالا وهندوراس وجامايكا والمكسيك ونيكاراغوا وبنما وباراغواي وبيرو وأوروغواي وفنزويلا (جمهورية فنزويلا البوليفارية).

١- المقدمة

١-١ أدى الاستخدام المتزايد لأحدث التقنيات المترابطة عالمياً في مجال الطيران المدني إلى زيادة ملحوظة في مخاطر التهديدات التي تأتي عن طريق الإنترنت.

١-٢ أقرت الجمعية العمومية للإيكاو في دورتها الحادية والأربعين بأهمية هذه المسألة من خلال إدراج قرار الجمعية العمومية ٤١-١٩: ***معالجة الأمن الإلكتروني في مجال الطيران المدني*** في ***القرارات السارية المفعول الصادرة عن الجمعية العمومية (في ٧/١٠/٢٠٢٢)*** (الوثيقة Doc 10184)، الجزء السابع – ***التدخل غير المشروع؛ شؤون أخرى متعلقة بالتدخل غير المشروع***. ودعت الدول إلى اتخاذ عدد من الإجراءات؛ وينبغي اتخاذ بعض هذه الإجراءات باستخدام الأدوات التنظيمية، بحيث تتاح معالجة الشواغل الحالية في مجتمع الطيران بشأن فعالية القواعد القياسية والإجراءات والعمليات الحالية عندما يتعلق الأمر بالحفاظ على مستوى مقبول من المخاطر في بيئة متصلة رقميا.

١-٣ وفقاً لمقال نشرته مجموعة أليانز في عام ٢٠١٩ بعنوان "مقياس المخاطر: أهم مخاطر مؤسسات الأعمال" (مقتبس من الطبعة السابعة من الخطة العالمية للملاحة الجوية (Doc 9750))، فإن أكثر أنواع انقطاع الأعمال إثارة للرعب هي الهجمات الإلكترونية القائمة على برمجيات انتزاع الفدية[٣]. وتعد برمجيتا WannaCry وPetya مثالين على برمجيات انتزاع الفدية المستخدمة لمهاجمة النظم الرقمية في الاتحاد الأوروبي. ومع ذلك، من المثير للاهتمام تسليط الضوء على أن المقال يذكر أن ١٢ في المائة من عمليات تحليل المعلومات المتعلقة بالأعمال تحدث نتيجة لهجمات إلكترونية إجرامية، بينما تُجرى نسبة ٨٨ في المائة منها نتيجة لأعطال تقنية أو أخطاء ناجمة عن تفاعل الإنسان مع النظم.

١-٤ وبذلت جميع الجهات المعنية بالطيران المدني جهوداً تعاونية كبيرة لصون شبكة الملاحة الجوية وحمايتها من أعمال التدخل غير المشروع، مع إعطاء الأولوية لإدارة المخاطر وقدرة الشبكة الإلكترونية على الصمود. وفي هذا السياق، تؤدي الهيئات التنظيمية للطيران المدني دوراً أساسياً ينبغي أن يستمر في التطور. وهذا يعني أنه بالإضافة إلى اللوائح المعمول بها حالياً، سيكون من المفيد تقديم ابتكارات مرنة وقابلة للتطوير، لا سيما في ضوء نماذج الأعمال الجديدة قيد الإعداد التي ينبغي أن يكون التركيز فيها على الأعمال التجارية من المؤسسة إلى المؤسسة و/أو من المؤسسة إلى المستهلك[٤]. وبناء على ذلك، ينبغي أن تحدد اللوائح قواعد الأداء القياسية اللازمة لهذا السياق الجديد بدلاً من الاحتفاظ بوظيفتها السابقة المتمثلة في تحديد فرادى العناصر التقنية بتفصيل مستفيض.

١-٥ ولذلك، ينبغي أن تيسر اللوائح الابتكار وتعززه، وأن تفي بمتطلبات الأداء، وأن تدعم تطور شبكة الملاحة الجوية، مع ضمان الرصد والمراقبة في الوقت نفسه. ومن وجهة النظر هذه، يمثل النموذج التنظيمي الجديد من نواح كثيرة انتقالاً من نظام مركزي مصمم لجهتين فاعلتين فقط (الهيئة التنظيمية الحكومية ومقدم خدمات الملاحة الجوية) إلى نظام لوائح موزع ومنسق يقدم خدمات تتكيف مع احتياجات البنية الأساسية الإلكترونية القادرة على الصمود والاحتياجات المحددة للمستخدمين.

٢- المناقشة

---

[٣] برامج انتزاع الفدية هي نوع من البرمجيات الخبيثة التي تقوم بتشفير محفوظات المستخدم ثم تطلب فدية لاستعادتها.

[٤] الخطة العالمية للملاحة الجوية المتاحة على شبكة الإنترنت. نماذج الأعمال الناشئة والجديدة والمكيفة، الإيكاو: https://www4.icao.int/ganpportal/GanpDocument#/lessons/WWfUWzbjlhwCVRRkMTd9NRWaFjpHfZxp

٢-١ على ضوء ما سبق، نقدم عدداً من الاعتبارات التي تعزز مواءمة واتساق الأحكام التنظيمية لخدمات الحركة الجوية. وهدفنا هو تحليل المقترح لتضمينه المواصفات والإجراءات ذات الصلة بسيناريوهات الهجمات المحتملة للبرمجيات الخبيثة ضد نظم المعلومات، مع تلبية احتياجات جميع الجهات المعنية وتوفير المراقبة المستمرة للتدريب الأولي والتدريب لتجديد المعارف من أجل ضمان حفاظ الموظفين على المهارات اللازمة.

٢-١-١ ويصنف سيناريو الهجوم الإلكتروني ضد الطيران المدني على أنه تدخل غير مشروع وفقاً لقرار الجمعية العمومية ٤١-١٩: ***معالجة الأمن الإلكتروني في مجال الطيران المدني*** وبسبب طبيعته الإجرامية.

٢-١-٢ وتهدف أوجه التقدم التكنولوجي والترابط بين شبكات الملاحة الجوية إلى تحقيق السلامة، ولكنها قد تهيئ الظروف التي يمكن أن يُحدث فيها التدخل غير المشروع آثاراً لا تقع على الطائرة فحسب، بل تقع أيضاً على النظم التابعة لخدمات الحركة الجوية.

٢-١-٣ وإن القواعد والتوصيات الدولية الواردة في الملحق الحادي عشر لاتفاقية الطيران المدني الدولي — ***خدمات الحركة الجوية***، والأساليب المبيّنة في ***إجراءات خدمات الملاحة الجوية - إدارة الحركة الجوية*** (الوثيقة Doc 4444)، تتناول التدخل غير المشروع من خلال الأفعال أو الإجراءات إذا كانت الطائرة هدفاً لتدخل غير مشروع أو يشتبه في أنها كذلك.

٢-١-٤ ولا تتناول الوثيقتان المذكورتان آنفاً حالة وقوع هجوم محتمل على النظم التابعة لخدمات الحركة الجوية. ولذلك، قد يكون من الضروري إدراج الإرشادات التنظيمية أو التقنية للإيكاو في النظم التابعة لخدمات الحركة الجوية المتأثرة بالهجمات الإلكترونية من أجل توفير إجراءات مناسبة للتصدي لمثل هذه الأحداث. ونقترح دراسة سيناريو التدخل غير المشروع في خدمات الحركة الجوية من أجل وضع تدابير محددة لمكافحة الهجمات الإلكترونية.

٢-١-٥ وانطلاقاً من هذه الاعتبارات، ووفقاً لخطة عمل الأمن الإلكتروني الخاصة بالإيكاو، نقترح تحليل ما إذا كان من الممكن إدراج مواصفات و/أو إجراءات لإخطار السلطة المختصة التي عينتها الدولة بالحالات التي يشتبه في أنه وقع فيها هجوم إلكتروني على أحد النظم التابعة لخدمة الحركة الجوية، أو تأكد وقوع هذا الهجوم، مما يتيح تبادل المعلومات ذات الصلة بالواقعة في الوقت المناسب بين جميع الجهات المعنية، ولا سيما المشغلين الجويين.

٢-١-٦ وفضلاً عن ذلك، نعتقد أنه قد يكون من الضروري إنشاء آليات لتبادل معلومات الأمن الإلكتروني بين السلطات العسكرية وخدمة الحركة الجوية بحيث يتسنى تبادل المعلومات في هذا الشأن. فلعل هذا النهج التعاوني يسهم في التخفيف من مخاطر الهجمات الإلكترونية في خدمات الحركة الجوية.

٢-٢ وبالإضافة إلى ذلك، واستناداً إلى أن خطة عمل الأمن الإلكتروني تشير إلى ضرورة "السعي إلى تحقيق الاتساق التنظيمي على المستوى العالمي والإقليمي والوطني من أجل تعزيز الترابط العالمي وضمان قابلية التشغيل البيني لتدابير الحماية"[٥]، نلاحظ أن هناك حاجة إلى إدراج أحكام تنظيمية محددة، دون الإخلال باعتماد أحكام أخرى تتعلق بهذه المسألة، ومنها ما يلي:

[٥] خطة عمل الأمن الإلكتروني، الفصل ٣، خطة العمل الاستراتيجية، الركيزة ١: التعاون الدولي، الإيكاو، طبعة عام ٢٠٢٢.

أ) إجراءات تعالج سيناريوهات التهديد الإلكتروني والهجمات الإلكترونية على المستوى الإقليمي، لأن من شأن ذلك أن يوفر وسيلة لمعالجة أوجه الاختلاف الاقتصادية والتكنولوجية التي تعالجها بعض الدول بمفردها، لا سيما إذا روعي أن تأثير الهجوم الإلكتروني أو التهديد الإلكتروني يتجاوز عادة حدود الدول؛

ب) أدوات ملائمة لتوفير الربط بين استراتيجية الأمن الإلكتروني للدولة والمبادئ التوجيهية للإيكاو المنصوص عليها في استراتيجية الأمن الإلكتروني في مجال الطيران، مما يضمن أن يوفر الطيران المدني المحلي سياسة واستراتيجية وتدريباً، والتكاليف المرتبطة بتنفيذ هذه الاستراتيجية. وسيتضمن ذلك أيضاً تعيين السلطة المختصة بالأمن الإلكتروني للطيران المدني وبيان كيفية تفاعل هذه السلطة مع المؤسسات الوطنية والجهات المعنية الأخرى المهتمة بالأمر؛

ج) أحكام تتعلق بأمن نظم الملاحة الجوية الحكومية، وتقترن ببنية تضمن سلامتها وحمايتها. ويمكن أن يشمل ذلك أساليب الإبلاغ والمراقبة وإجراء تحليلات علم الأدلة الجنائية[٦] للوقائع الإلكترونية الخاصة بالطيران المدني؛

د) أحكام تتعلق بالتدريب لتعزيز ثقافة الأمن الإلكتروني في خدمة الحركة الجوية وتوفير التدريب الملائم لجميع الموظفين العاملين في شبكة الملاحة الجوية. ومن هذا المنطلق، سيكون من الضروري وضع أحكام بشأن الاضطلاع بمشاريع لتدريب الموظفين المذكورين؛

هـ) تدابير طوارئ محددة في خدمات الحركة الجوية لمعالجة هذه الحالات وضمان التعافي السريع للعمليات، بما في ذلك إجراءات التعافي من الوقائع الإلكترونية وتحديد الجهات المعنية الرئيسية من أجل ضمان الفعالية في التواصل والتنسيق أثناء الأزمات؛

و) بروتوكولات للكشف عن الوقائع الإلكترونية والإبلاغ عنها ووضع إجراءات واضحة للكشف المبكر والإبلاغ في الوقت المناسب عن أي حادث أمن إلكتروني يؤثر في النظم التابعة لخدمة الحركة الجوية. ومن شأن هذا الأمر أن يضمن تصدياً سريعاً ومنسقاً لأي تهديد، والحد بذلك من الأثر المحتمل للهجمات الإلكترونية على سلامة عمليات الطيران واستمراريتها.

٣- الاستنتاجات

٣-١ يمثل الأمن الإلكتروني في خدمات الحركة الجوية شاغلاً يستلزم اتخاذ إجراءات منسقة على المستوى الوطني والإقليمي والعالمي. ويعد الأخذ بالمقترحات الواردة في هذه الورقة خطوة مهمة نحو تعزيز أمن الخدمة والتخفيف من المخاطر المرتبطة بالهجمات الإلكترونية في النظم التابعة لخدمة الحركة الجوية. وباعتماد هذه النهوج، ستكون الدول أكثر استعداداً لمواجهة تحديات الأمن الإلكتروني الناشئة، مع ضمان استمرارية وسلامة عمليات الطيران في الوقت نفسه. وبالإضافة إلى ذلك، سيساهم التعاون الدولي والاتساق التنظيمي في تعزيز ثقافة الأمن الإلكتروني القوية والقادرة على الصمود في مجتمع الطيران العالمي برمته.

٣-٢ لذلك، يرجى من المؤتمر الموافقة على التدبيرين التاليين:

---

[٦] تحليل الأمن الإلكتروني استناداً إلى علم الأدلة الجنائية هو تخصص يستخدم للتحقيق في وقائع أمن المعلومات وتحليلها. وتشمل هذه الوقائع الهجمات الإلكترونية وسرقة البيانات والاقتحامات.

أ) دعم المبادرات المعروضة في ورقة العمل هذه، مع طلب إجراء تحليل لفائدة إدراج لوائح وأساليب الأمن الإلكتروني الخاصة بخدمات الحركة الجوية في إطار الطيران العالمي؛

ب) تشجيع الدول على دمج استراتيجياتها الوطنية للأمن الإلكتروني مع استراتيجيات الإيكاو بشأن الطيران المدني من أجل إقامة ثقافة أمن إلكتروني في مجال خدمات الحركة الجوية وإدراج السياسات والاستراتيجيات والآليات بوصفها ضمانات، من خلال وضع الأحكام التنظيمية المقترحة.

— انتهى —