AN-Conf/13-WP/42
28/8/18

منظمة الطيران المدني الدولي

ورقة عمل

المؤتمر الثالث عشر للملاحة الجوية

مونتريال، كندا، من ٩ إلى ٢٠١٨/١٠/١٩

اللجنة (أ)

البند ٥ من جدول الأعمال: القضايا الناشئة

البند الفرعي ٥-٤: تحصين الشبكة الإلكترونية

تعزيز مفاهيم الأمن الإلكتروني في مجال الطيران

(ورقة مُقدَّمة من النمسا باسم الاتحاد الأوروبي ودوله الأعضاء[١] والدول الأخرى الأعضاء في المؤتمر الأوروبي للطيران المدني[٢]، ومن المنظمة الأوروبية لسلامة الملاحة الجوية (يوروكنترول))

الموجز التنفيذي

ستعرض هذه الورقة بإيجاز الأسس المنطقية التي تدفع المنظمات إلى إدارة فرادى مخاطرها ومنتجاتها وخدماتها في مجال الأمن الإلكتروني من خلال نظام إدارة أمن المعلومات (ISMS) الذي يراعي المخاطر المتعلقة بتفاعلات المنظمة مع المنظمات الأخرى أو النُظم التي تديرها.

وتركز الورقة أيضاً على الجدارة بالثقة (الاعتمادية/الموثوقية)، والداعي إليها، والفوائد التي توفرها للمنظمات عند استخدام نظام لإدارة أمن المعلومات. كما تتناول الورقة بالإضافة إلى ذلك أهمية وجود مستوى مكافئ من الأداء المتعلق بالأمن الإلكتروني للأنظمة المتصلة ببعضها، بمعزل عن الزمان والمكان، كشرط أساسي وكيفية تحقيق ذلك للعمليات الأرضية/الأرضية أو الجوية/الأرضية.

وتطرح الورقة فوق ذلك منظوراً مشتركاً لفوائد تقاسم المعلومات وأهميته البالغة في مجال الطيران.

الإجراء المطلوب: المؤتمر مدعوٌ إلى الموافقة على التوصيات الواردة في الفقرة رقم ٣.

١- المقدمة

١-١ يُعتبر توافر المعلومات الدقيقة والأداء السليم للنُظم الحساسة من حيث السلامة شرطين مسبقين لسلامة الطيران المدني وأمنه نظراً لأن القطاع بصدد المزيد من التوجه نحو الرقمنة. ويتسم نظام الطيران بالتكامل الشديد وتنقُّل المعلومات فيه على الصعيد العالمي. ولذلك، فإنه يجب اتباع نهج شمولي من الطرف إلى الطرف لمبادرات الأمن الإلكتروني في قطاع الطيران.

[١] إسبانيا، إستونيا، ألمانيا، آيرلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، بولندا، الجمهورية التشيكية، الدانمرك، رومانيا، سلوفاكيا، سلوفينيا، السويد، فرنسا، فنلندا، قبرص، كرواتيا، لاتفيا، ليتوانيا، لكسمبرغ، مالطة، المملكة المتحدة، النمسا، هنغاريا، هولندا، اليونان.

[٢] أذربيجان، أرمينيا، ألبانيا، أوكرانيا، آيسلندا، البوسنة والهرسك، تركيا، الجبل الأسود، جمهوريه مقدونيا اليوغوسلافية السابقة، جمهورية مولدوفا، جورجيا، سان مارينو، سويسرا، صربيا، موناكو، النرويج.

١-٢ تسلط هذه الورقة الضوء على مزايا إدخال نُظم إدارة أمن المعلومات إلى قطاع الطيران. فمثل هذه النُظم، التي يُفضّل مواءمتها أو دمجها مع النُظم القائمة لإدارة مخاطر الطيران، تساعد فرادى المنظمات والقطاع ككل على التأهب والتصدي بشكل أفضل للتهديدات المتعلقة بأمن المعلومات.

١-٣ يتيح نهج نظام الإدارة المشترك تنسيق التدابير على نطاق القطاع، مع مراعاة أنه يجري تقاسم المعلومات، وأن النظم في حد ذاتها مشتركة بين العديد من الجهات الفاعلة في القطاع، وأن المخاطر مشتركة أيضاً.

١-٤ بالإضافة إلى نهج نُظم إدارة أمن المعلومات، تتناول هذه الورقة بالتفصيل أيضاً مفهوم الثقة. ففي قطاع الطيران، تشكل الثقة في كل شريك أمراً بالغ الأهمية. ويضمن وجود نظام قوي للتدريب والترخيص والمراقبة والفحص المزدوج، لكل رحلة، الثقة فيما بين الشركاء بشأن وفاء كل منهم بدوره ضمن سلسلة الطيران بشكل واعٍ وصحيح.

٢- المناقشة

٢-١ **كيفية الاستفادة من نُظم إدارة أمن المعلومات** – تقتصر المفاهيم الحالية لنُظم إدارة أمن المعلومات بطبيعتها على فرادى المنظمات. ومع ذلك، يعتبر نظام الطيران المدني نسيجاً من أنظمة متلاحمة، حيث يتألف من منتجات وأشخاص وعمليات يترابط بعضهم ببعض، بما في ذلك الاتصالات بالنظم العسكرية[٣]، ما يجعل بالتالي منظور فرادى المنظمات غير كافٍ. وعلى هذا النحو، فسيتعين على الطيران المدني أن يقدم نُظم إدارة أمن المعلومات من منطلق إدارة الأمن الإلكتروني عبر المنظمات.

٢-٢ وبالتالي فإن نهج تنسيق إدارة أمن المعلومات على الصعيد العالمي يُعد عاملاً تمكينياً رئيسياً لقطاع الطيران المدني. ومن شأن هذا الإطار العالمي أن يُسهل التنفيذ المتسق لعدد من المفاهيم الداعمة، مثل البنى الأساسية للاتصالات المؤمَّنة القابلة للتشغيل البيني عالمياً، فضلاً عن إطار الثقة أو المفاهيم الأخرى التي تسمح بنظام مستقبلي يستند إلى تبادل المعلومات الجدير بالثقة. ونظراً لأن المستقبل لا يُبنى في وقت واحد، فسيكون من الضروري تسهيل تطور فرادى المنظمات أو الدول أو الأقاليم. وسيكون وجود نُظم لإدارة أمن المعلومات في جميع المنظمات شرطاً مسبقاً لجعل تلك المفاهيم حقيقة واقعة. وينبغي أن تتماشى تطبيقات نُظم إدارة أمن المعلومات مع نُظم إدارة السلامة القائمة (على سبيل المثال، الملحق التاسع عشر – *إدارة السلامة*) وإدارة المخاطر وأحكام الإيكاو ومعايير الصناعة المتعلقة بأمن الطيران فضلاً عن آليات المراقبة الفعالة.

٢-٣ **مفهوم الجدارة بالثقة (الاعتمادية/الموثوقية)** – فيما يتعلق بالطيران المدني، تم بناء إطار قوي للثقة على مدى عقود. وأصبحت الجدارة بالثقة الآن مفهوماً رسمياً يمكن لمنظمة ما – أو لأحد نظمها – الاعتماد على خصائص الأمن الإلكتروني لمنظمة أخرى – أو أحد نظمها[٤]. وبما أن الثقة ليست مطلقة أبداً، فإن هذا المفهوم يقترح مستويات متعددة من الموثوقية، اعتماداً على تأثير (السلامة أو استمرارية الخدمة، مثل التدفق السريع للحركة الجوية في أحد الأقاليم) ذلك في الطرف المُعوّل.

٢-٤ على سبيل المثال، فيما يتعلق بترخيص الطائرة، يكون معظم الثقة في صلاحية الطائرة للطيران مستمداً من الاطمئنان إلى أن الإجراءات المناسبة قد نُفِّذت وأسفرت عن نتائج مقبولة. وقد صممت هذه الإجراءات لمعالجة شدة تأثير مخاطر السلامة. أما مستويات شدة التأثير الأعلى، فستحتاج إلى مستويات أعلى من التمحيص في عملية التطوير. وفيما يتعلق بخصائص الأمن الإلكتروني، فثمة مفهوم مماثل مقترح. وهو مصمم بحيث يعكس فعالية الحماية من التهديدات الإلكترونية. وفي الأساس، فإن الثقة مع غياب الأخطاء ونقاط ضعف التطوير ومع تمكن المنظمات من توفير الحماية الكافية للطيران المدني هي التي ستُعد مستقبل الطيران الآمن. وينبغي إدماج مفهوم الجدارة بالثقة في نظام إدارة أمن المعلومات، الذي ينبغي بالتالي مواءمته أو دمجه مع نُظم الإدارة القائمة.

---

[٣] يرجى الاطلاع على الوثيقة AN-Conf/13-WP/39

[٤] تقدم ورقة المعلومات (AN-Conf/13-WP/160) شرحاً لمفاهيم ومبادئ نُظم إدارة امن المعلومات، والموثوقية، ومفاهيم أوضاع تشغيل الأمن الإلكتروني، فضلاً عن فوائد تقاسم المعلومات.

٢-٥ **أوضاع تشغيل الأمن الإلكتروني** – من أجل الاستفادة الكاملة من مفهوم الجدارة بالثقة (الموثوقية)، يجب أيضاً تغطية ديناميات تطور فرادى المنظمات ونظمها، ووجود البنى الأساسية المؤمّنة القابلة للتشغيل البيني على الصعيد العالمي. وتجدر الإشارة إلى أن أوضاع تشغيل الأمن الإلكتروني المحددة مسبقاً هي إحدى الطرق للتصدي لهذا التحدي. ولكل وصلة بين قرينين، سيكون من الضروري توافق مستويات الجدارة بالثقة فيما بينهما، ما يتطلب بالتالي تعريف الأزواج المتطابقة. وسوف يُسمح بالربط بين توليفات معينة من المزاوجة بين مستويات الجدارة بالثقة إذا كانت تفي بأهداف الأمن الإلكتروني مع وجود مستويات مقبولة من المخاطر. بينما قد تخفق توليفات أخرى في تحقيق الأهداف. وذلك سيخلق دوافع للتوصل إلى اتفاقات بين الأقران بشأن الشروط المتعلقة بمستويات الثقة المتوافقة وإن كانت متباينة، والتي ستؤدي في نهاية المطاف إلى نهوج متوازنة. وينبغي التمييز بين مستويين من الانتقال بين الوصلات فيما بين الأقران: المستوى بين المنظمات التي تربط نُظمها، والمستوى بين المركبات الجوية أو الفضائية والنُظم الأرضية، التي يكون الانتقال فيها بين الوصلات بوتيرة سريعة. ووجه التمايز الرئيسي لديها هو سرعة تطور وضع الأمن الإلكتروني.

٢-٦ التطور البطيء: من ناحية، تتطور النظم الأرضية بشكل عام – وإدارة الحركة الجوية/خدمات الملاحة الجوية على وجه الخصوص – بوتيرة بطيئة نسبياً. وتتحدد التغييرات في وضع التشغيل الخاص بها إلى حد كبير عن طريق التغييرات إما في وضع الأمن الإلكتروني الخاص بهم، وإما في النظم المتصلة بها. وهذا يسمح بتكييف خصائص الأمن الإلكتروني المنسق بشكل وثيق بحيث تتمكن جميع الأطراف المتصلة من تلبية متطلبات الأمن الإلكتروني الشاملة. ويعالج مفهوم أوضاع التشغيل المزاوجة المناسبة بين مستويات الجدارة بالثقة بين المنظمات المتصلة ببعضها.

٢-٧ التطور السريع: ومن ناحية أخرى، تنتقل الطائرات من موقع إلى آخر بوتيرة عالية نسبياً، بينما تتصل دينامياً بعدد كبير من الأقران خلال فتره قصيرة من الزمن. وبصفة عامة، فإن الطائرات أو نظم إدارة الحركة الجوية/خدمات الملاحة الجوية لن تكون في حالة مطابقة من حيث الأمن الإلكتروني في يوم واحد معين. ومن أجل الإبقاء على جاهزيتها التشغيلية، سيكون من الضروري الانتقال على أي من الجانبين. وفيما يتعلق بالأمن الإلكتروني، فإن تكييف مفهوم وضع التشغيل يمكن أن يعطي استجابة. فعلى سبيل المثال، في المفهوم الحالي لأوضاع التشغيل، تقتضي متطلبات الفصل الأفقي المطبقة داخل أحد المجالات الجوية وجود تجهيزات معينة للنُظم الأرضية ونُظم الطائرة لتلبية هذه الاحتياجات. وبالتالي فإن مفهوم أوضاع التشغيل يمكن أن يكون بمثابة مخطط الأمن الإلكتروني الذي يتولى الاستجابة للمتطلبات المتعلقة بخصائص الأمن الإلكتروني التي قدمتها مستويات الجدارة بالثقة. ومن شأن مزاوجة مستويات الجدارة بالثقة بشكل مناسب بين إدارة الحركة الجوية/خدمات الملاحة الجوية ونُظم الطائرات أن تسمح باستخدام المجال الجوي بشكل يراعي السلامة والأمن.

٢-٨ **تقاسم المعلومات بشأن الجوانب الإلكترونية** – ثمة جانب آخر يتعين النظر فيه كجزء من نظام إدارة أمن المعلومات، وهو تقاسم المعلومات. كما يمكن للإطار العالمي لنظام إدارة أمن المعلومات أن يساعد على وضع آليات أكثر تماسكاً لتقاسم المعلومات بشأن مخاطر الأمن الإلكتروني. وقد أوجد عالم تكنولوجيا المعلومات مفهوم مركز الأمن الإلكتروني الذي "يعالج" المعلومات بشأن وقائع الأمن الإلكتروني، بما في ذلك جمع وصيانة قواعد بيانات الحوادث والتهديدات ومواطن الضعف، وتقديم تحليلات وإرشادات إلى المعنيين بشأن الممارسات الناجحة في مجال كيفية التصدي للوقائع الفعلية في هذا الصدد. وترتبط هذه المهام بتقاسم المعلومات.

٢-٩ وعلى الصعيد الدولي، أنشأت أفرقة الاستجابة لطوارئ الحواسيب (CRETs) وأفرقة الاستجابة للوقائع المتعلقة بأمن الحواسيب (CSIRTs) محفلاً اسمه منتدى أفرقة الاستجابة للوقائع الأمنية (FIRST) الذي يمكنه خدمة أوساط الطيران كمخطط لنهج متناغم لتقاسم المعلومات على الصعيد العالمي ليس بهدف الاستجابة للوقائع فحسب، بل أيضاً منع نجاح الهجمات في المستقبل. وفيما يتعلق بالتعامل مع اكتشاف نقاط ضعف جديدة، فسوف تسمح المعلومات التي جمعتها أفرقة الاستجابة للوقائع المتعلقة بأمن الحواسيب بتوقع بعض المخاطر الناشئة وبالتالي اتخاذ تدابير وقائية للحد من تأثيراتها الضارة في مجال الطيران المدني. وباختصار، فإن الغرض من هذا الهدف هو تحسين الوعي بالتهديدات الإلكترونية ومواطن الضعف في نظم الطيران. وبمجرد أن تنسق أفرقة الاستجابة للوقائع المتعلقة بأمن الحواسيب فيما بينها وبين أعضاء كل منها، سيكون من الممكن اتخاذ تدابير مُنسّقة دولياً للتخفيف من التهديدات الإلكترونية ومواجهتها.

٢-١٠ تجدر الإشارة إلى أن تهديدات الأمن الإلكتروني تتجاوز مجال الطيران المدني، على سبيل المثال، إلى قطاعات النقل الأخرى وإلى غير قطاعات النقل أيضاً (كالنُظم المصرفية والصناعة النووية). فكثيراً ما تتقاسم تلك المجالات التكنولوجيات والتطبيقات ذاتها، وبالتالي، فهي تتقاسم التهديدات ومواطن الضعف ذاتها. ولذلك فمن الأساسي تبادل السياسات والمعلومات الاستخباراتية وأفضل الممارسات مع المنظمات التي تنتمي إلى مثل هذه القطاعات. وبالتالي، ينبغي أن يستفيد نهج الأمن الإلكتروني في مجال الطيران المدني من الخبرات والنهوج الشاملة لعدة قطاعات على الصعيدين الوطني أو الإقليمي. وعلاوة على ذلك، فان الاتصال الوثيق مع الكيانات الحكومية المنخرطة في الأمن الإلكتروني في القطاعات الأخرى سيعزز الفوائد التي تعود على سلطات الطيران المدني في الدول.

٣- الاستنتاج

٣-١ إن المؤتمر مدعوّ إلى الموافقة على التوصيات التالية:

أن يقوم المؤتمر بما يلي:

أ) يحث الإيكاو على دعم الدول في مطالبة المنظمات بإدارة مخاطر الأمن الإلكتروني المتعلقة بعملياتها ومنتجاتها وخدماتها، بما في ذلك الوصلات البينية للأقران، عن طريق نظام إدارة أمن المعلومات، استناداً إلى معايير الصناعة الدولية ويفضل مواءمتها أو دمجها مع نظم الإدارة القائمة؛

ب) يطلب إلى الإيكاو أن تشجع الدول على اتخاذ التدابير المناسبة التي تكفل وجود بنى أساسية قابلة للتشغيل البيني على الصعيد العالمي، وقادرة على التصدي للهجمات الإلكترونية وتلبية متطلبات القابلية التشغيل البيني والأمن الإلكتروني من أجل تعزيز الأهداف الكلية والأعلى مستوى فيما يتعلق بالسلامة والتدفق السريع للحركة الجوية؛

ج) يحث الإيكاو على أن تضع، باتباع نهج متعدد التخصصات، أحكاماً للثقة المشتركة بين المنظمات، كجزء من إطار أوسع نطاقا للثقة، وأن تشجع على تنفيذها؛

د) يطلب إلى الإيكاو أن تشجع الدول على اتخاذ تدابير، بحيث يقوم المشغلون الجويون بإجراء وتسهيل تقاسم المعلومات التشغيلية المتصلة بالأمن الإلكتروني من خلال القنوات المحددة على النحو المناسب، كشبكة عالمية من "منظمات موثوق بها"؛

هـ) يحث الإيكاو على تسهيل وضع أحكام تتعلق بالجدارة بالثقة وأوضاع تشغيل الأمن الإلكتروني للسماح بتشغيل هذه البنى الأساسية القابلة للتشغيل البيني العالمي بشكل مؤمَّن؛

و) يطلب إلى الإيكاو أن تشجع الدول على توسيع القنوات القائمة، أو إنشاء قنوات جديدة، للإبلاغ عن الوقائع المتصلة بالأمن الإلكتروني، وذلك من أجل تحسين معالجة المخاطر الجديدة في مجال سلامة الطيران وأمنه وضمان التدفق السريع للحركة الجوية؛

ز) يطلب إلى الإيكاو أن تدعو الدول إلى تعزيز التعاون الحكومي وغير الحكومي الشامل لعدة قطاعات بشأن الأمن الإلكتروني بين مجالات الطيران والمجالات الأخرى.

– انتهى –