خطة عمل الأمن الإلكتروني

نشرت بموجب سلطة الأمين العام

الطبعة الثانية، يناير ٢٠٢٢

منظمة الطيران المدني الدولي

المصطلحات والتعاريف[1]

نظام إدارة أمن المعلومات في الطيران المدني (caISMS):

نموذج لإنشاء رصيد المعلومات وتنفيذها وتشغيلها ورصدها ومراجعتها وتحديثها وتحسين حمايتها من أجل تحقيق أهداف الطيران المدني على أساس تقييم للمخاطر ومستويات المنظم لقبول المخاطر المصممة لمعالجة المخاطر وإدارتها. المرجع القاعدة ISO27000:2009 الصادرة عن المنظمة الدولية لتوحيد المقاييس.

الأمن الإلكتروني:

مجموعة من الأساليب والتقنيات والضوابط والتدابير والعمليات والممارسات المصممة لضمان السرية والسلامة والإتاحة والحماية بشكل شامل للأنظمة والشبكات والبرامج والأجهزة والمعلومات والبيانات ضد الهجمات والتلف، وضد الوصول و/أو الاستخدام و/أو الاستغلال دون الحصول على تصريح بذلك.

سياسة الأمن الإلكتروني:

توثق سياسة الأمن الإلكتروني النوايا وتوجه أي منظمة لإدارة تهديدات الأمن الإلكتروني، كما يتم الإعراب عنها من جانب الإدارة العليا. وهي تتمثل في وثيقة مكتوبة في منظمة ما تحدد فيها كيفية حماية المنظمة من التهديدات الإلكترونية وكيفية معالجة الوقائع والأحداث متى حدثت.

أحداث

تعرّض النظم أو الخدمات أو الشبكات لحالة تشير إلى وقوع خرق مُحتمل لسياسة أمن المعلومات أو إلى حدوث فشل في المراقبة أو وضع غير معروف مسبقاً قد يتعلق بالأمن. [القاعدة القياسية ISO/IEC 27035 الصادرة عن المنظمة الدولية لتوحيد المقاييس]. وتجدر الإشارة إلى ضرورة فهم الحدث بمعناه الأشمل، ولا يجب اعتباره مصطلحاً يعبر عن حدث يتعلق (بالسلامة) ويقتصر فقط على الأنشطة التي تكتسي أو قد تكتسي أهمية في سياق سلامة الطيران.

وقائع

هي عبارة عن حدث أو سلسلة من الأحداث غير المرغوبة أو غير المتوقعة المرتبطة بأمن المعلومات والتي تنطوي على احتمالات كبيرة لتعريض أنشطة تسيير الأعمال للخطر فضلا عن تهديد أمن المعلومات. [القاعدة القياسية ISO/IEC 27035-1 الصادرة عن المنظمة الدولية لتوحيد المقاييس].

أمن المعلومات

الحفاظ على سرية المعلومات وسلامتها وتوافرها. فضلا عن ذلك، يمكن أن تضاف خصائص أخرى مثل الصحة والمساءلة وعدم الإنكار والموثوقية. [انظر معيار ISO/IEC 27000:2018].

تبادل المعلومات

العملية التي يتم من خلالها تقديم المعلومات من قبل كيان واحد إلى كيان أو أكثر لتسهيل اتخاذ القرارات القائمة على المخاطر وتعزيز أفضل الممارسات.

مصفوفة المخاطر

أداة لترتيب عناصر المخاطر وعرضها (التهديد واحتمال وقوعه وتأثيره/عواقبه ومواطن الضعف) والإجراءات المُتَّخذة للتخفيف من المخاطر والإشارة في نهاية المطاف إلى المخاطر المتبقية.

كيان مُهدِّد (أو جهة فاعلة)

الكيان المسؤول، بشكل جزئي أو كامل، عن أي واقعة تؤثر، أو يحتمل أن تؤثر، في أي منظمة أو نظام.

---

[1] قيد الاستعراض.

مواطن الضعف

ضعف في نظام معلومات أو في إجراءات أمن النظام أو في ضوابط داخلية أو في خطوات تنفيذ، بشكل يمكن استغلاله أو توظيفه من قبل كيان مهدِّد. وقد يكون ذلك نظاماً يدعم بشكل مباشر أو غير مباشر وظيفة من وظائف منظومة الطيران.

الموجز التنفيذي

أعادت الجمعية العمومية للإيكاو خلال دورتها التاسعة والثلاثين التأكيد على الطابع الهام والمُلحّ لحماية نُظم وبيانات البنى التحتية الحساسة في مجال الطيران المدني ضدّ الهجمات الإلكترونية والحصول على التزام عالمي باتخاذ الإجراءات من جانب الايكاو والدول الأعضاء فيها والجهات المعنية في قطاع الطيران، وذلك بهدف العمل بشكل تعاوني ومنتظم على معالجة مشاكل الأمن الإلكتروني في مجال الطيران المدني والتخفيف من حدّة ما يترتب على ذلك من تهديدات ومخاطر. وقد حدّد القرار 19-39 "معالجة الأمن الإلكتروني في الطيران المدني" الإجراءات التي يتعين أن تتخذها الدول وغيرها من الجهات المعنية في هذا الصدد. كما قامت الجمعية العمومية للإيكاو خلال دورتها التاسعة والثلاثين بتكليف الإيكاو بوضع خطة عمل شاملة في مجال الأمن الإلكتروني.

وبهدف الوفاء بتوقعات الجمعية العمومية، أعدت المجموعة التابعة للأمانة العامة والمعنية بالأمن الإلكتروني استراتيجية الأمن الإلكتروني للطيران المدني.

وقد اعتمدت الدورة الأربعون لجمعية الإيكاو العمومية قرارا معدلا رقمه A40-10 بعنوان "معالجة الأمن الإلكتروني في الطيران المدني"، وطالبت فيه الدول تنفيذ استراتيجية الأمن الإلكتروني، مشددةً على أهمية إعداد خطة عمل مستدامة لتنفيذ هذه الاستراتيجية بالإضافة إلى مواصلة العمل على إعداد إطار قوي للأمن الإلكتروني.

وتتيح خطة عمل الأمن الإلكتروني الأساس للدول والقطاع والجهات المعنية والإيكاو للعمل يداً بيد من أجل تطوير قدرات التي تمكّن من تحديد الهجمات الإلكترونية ضد الطيران المدني وتجنبها والكشف عنها والتصدي لها والتعافي منها بالإضافة إلى خلق إطار صلب للتعاون. وقد أُعدت هذه الخطة بهدف اقتراح سلسلة من المبادئ والتدابير والإجراءات لتحقيق أهداف الركائز السبعة التي تستند إليها الاستراتيجية.

الفصل الأول

المقدمة

١-١ معلومات عامة

١-١-١ في السياق الحالي للطيران المدني، يُتوقع أن تزداد الحركة الجوية على المدى الطويل وأن تتطور التكنولوجيا بسرعة. كذلك فقد صارت العمليات أكثر تعقيدا، وبالتالي أصبحت البيئة التشغيلية مليئة بالتحديات. وتؤثر التغييرات التكنولوجية السريعة على طريقة تسيير الطيران المدني مما يجعل المنظومة أكثر هشاشة وعرضة لتهديدات الأمن الإلكتروني. ويمكن للنشاطات الإلكترونية الخبيثة أن تؤثر على الطيران المدني بوسائل وطرق عديدة، بدءا من الإخلال البسيط في العمليات إلى النتائج المأساوية. وتتنامى هذه المخاطر بسرعة، لذا ثمة حاجة ضرورية وملّحة لإعداد إطار مستدام للأمن الالكتروني على المستويات الوطنية والإقليمية والدولية.

١-١-٢ إن انشاء بنية أساسية متينة للأمن الالكتروني بالاعتماد على التعاون الوثيق والقوي فيما بين الدول والقطاع والإيكاو يتيح خلق الوعي المشترك بموضوع الأمن الإلكتروني، مما سيفضي في نهاية المطاف إلى نظام طيران مدني أكثر أمناً ومرونة.

١-١-٣ لا تتوقف الإيكاو عن التكيّف مع المستجدات لمواكبة المخاطر العالمية الآخذة في التطور، وذلك بالاتساق مع القرارات الصادرة عن مجلس الأمن للأمم المتحدة التي تؤكد على مسؤولية الدول عن ضمان سلامة الخدمات الجوية التي تعمل ضمن أقاليمها والتي تناشد جميع الدول للعمل مع الإيكاو من أجل ضمان مراجعة القواعد القياسية الدولية الأمنية وتحديثها وتنفيذها على أساس المخاطر الحالية ووفقا لاتفاقية شيكاغو. ومع تطور تهديدات الأمن الإلكتروني المتربصة بالطيران المدني والتي يُرجح ازدياد تواترها، وتبعا للأحكام التي ينص عليها قرار الصادر عن مجلس الأمن للأمم المتحدة ٢٣٤١ (عام ٢٠١٧)، تركز الإيكاو على إنشاء الآليات المناسبة للتخفيف من حدة المخاطر المتربصة بالبنية الأساسية الحرجة للطيران المدني الناتجة عن أفعال التدخل غير المشروع والحدّ منها عبر سبل الهجوم الإلكتروني والتصدي لأي حدث قد يؤثر في سلامة العمليات.

١-١-٤ وفي هذا الإطار، وبهدف تحقيق أهداف الركائز السبع التي تقوم عليها استراتيجية الأمن الإلكتروني بشكل سليم وإعداد إطار للأمن الإلكتروني في مجال الطيران، تم إعداد خطة العمل هذه.

١-٢ الغرض

١-٢-١ تعتبر هذه الخطة وثيقة حية تتطور مع التطورات الجارية في مجال الأمن الإلكتروني وستُحدّث بصورة منتظمة لإظهار التعديلات المطلوبة والناشئة عن نشاطات عديدة، من بينها تحاليل الثغرات ونشاطات وضع الجردات الواردة في الفصلين الثالث والرابع. وتحدد خطة عمل الأمن الإلكتروني الأهداف والتدابير التي ينبغي بلوغها لتنفيذ استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران. وتظهر العناصر المعروضة في هذه الوثيقة الأعمال المنجزة والجارية ضمن الأقاليم/الدول ومجالات القطاع المتعددة. وهي تشتمل على نتائج تحليل الوضع "القائم" لنظم الطيران من وجهة نظر الأمن الإلكتروني، مع مقارنته بالحالة "المتوخاة" المقترحة في الاستراتيجية، مع إعداد خطة عمل يمكن إلى أن تفضي إلى هذا التطور نحو الرؤيا الاستراتيجية.

١-٢-٢ نظرا للأعمال الهامة المطلوب إنجازها لتنفيذ الأهداف والإجراءات المحددة في هذه الوثيقة، يقترح في المرفق (أ) نهج مرحلي تحَدد فيه الأهداف على المدى القصير والمتوسط والطويل.

١-٣ سياق المخاطر

١-٣-١ لا يعتبر الأمن الإلكتروني مفهوما جديدا في مجال الطيران المدني. ولكن مع زيادة انتشار تهديدات الأمن الإلكتروني، فقد أصبح من الموضوعات الأساسية عند مناقشة وتحليل المخاطر المتربصة بنظام الطيران المدني وأوجه الهشاشة التي تشوبها. وإن قطاع الطيران المدني في خطر بصفة خاصة، لأنه من المرجح أن تنجح الهجمات الإلكترونية عندما تتعرض لقطاع تتطور فيه العناصر بطريقة تتسم باعتماد الواحد منها على الآخر وظيفياً ورقمياً، ولأن وسائل الدفاع الإلكترونية والتي تستخدم في قطاع الطيران المدني ليست قادرة بعد على معالجة هذا النوع من التهديد المستمر والآخذ في التطور.

١-٣-٢ أجرى فريق الإيكاو لخبراء أمن الطيران مؤخراً تقييماً لمستوى المخاطر الناشئة عن استغلال نقاط الضعف في سياق الإرهاب باعتبارها من المخاطر المتوسطة. وقد استند التقييم إلى أوجه الضعف المتبقية في مجال الأمن الإلكتروني على افتراض أن الدول قد نفذت أحكام الملحق السابع عشر "الأمن" تنفيذاً فعالاً. ولكن المخاطر الإلكترونية تتسارع في النمو، ويجب تقييمها بحيث يتم تغطية جميع فئات المهاجمين الإلكترونيين التي لا تؤثر فقط على سلامة عمليات الطيران المدني بل وعلى أمنه أيضاً. بالإضافة إلى ذلك، غالبا ما يكون من الصعب تحديد مصدر الهجمات الإلكترونية، وبالتالي فغالباً ما يكون تحديد مرتكبي الهجمات الإلكترونية وملاحقتهم أمراً معقداً ويصعب تحقيقه، في حين تتكبد ضحية الهجوم أو شركة التأمين المعنية بالتغطية التأمينية تكاليف التعافي من هذه الهجمات. ولهذا السبب، من الضروري بمكان أن تتعاون الإيكاو والدول والقطاع لتنفيذ استراتيجية الأمن الإلكتروني تتسم بالاتساق.

١-٤ منافع خطة العمل

١-٤-١ الهدف من خطة عمل الأمن الإلكتروني هو ضمان التزام كل من الإيكاو ودولها الأعضاء والقطاع بتنفيذ استراتيجية الأمن الإلكتروني في مجال الطيران وتحقيق الأهداف التي تنص عليها الركائز السبع. وإن اعتماد إطار صلب للأمن الإلكتروني من شأنه أن يعزز نظام الطيران المدني ويعود بالمنفعة على كامل أسرة الطيران في العالم.

الفصل الثاني

الهدف

٢-١ هدف خطة عمل الأمن الإلكتروني

٢-١-١ يكمن هدف خطة عمل الأمن الإلكتروني في تحقيق الأغراض المحددة في كل ركيزة من الركائز السبع للاستراتيجية إلى جانب إعداد إطار متين وصلب للأمن الإلكتروني في مجال الطيران المدني.

٢-١-٢ وترد المبادئ التي تشكل أساس خطة العمل الحالية كالتالي:

أ) فهم الدول الأعضاء لواجباتها فيما يخص الأمن الإلكتروني الناشئة عن اتفاقية الطيران المدني الدولي (اتفاقية شيكاغو) لضمان سلامة عمليات الطيران المدني وأمنها واستمراريتها؛

ب) تنسيق تدابير الأمن الإلكتروني للطيران فيما بين سلطات الدول الأعضاء لضمان الإدارة الفعالة والكفء على الصعيد العالمي للأمن الإلكتروني في مجال الطيران؛

ج) التزام جميع الجهات المعنية في مجال الطيران المدني بتعزيز المرونة الإلكترونية في وجه الهجمات الإلكترونية، وحماية الطيران منها، بصرف النظر عن شكل الكيان المُهدِّد الذي تنشأ عنه هذه الهجمات، والذي يمكن أن يؤثر على سلامة نظام النقل الجوي وأمنه واستمراريته.

٢-٢ التطبيق

٢-٢-١ تتوجه هذه الوثيقة أساسا إلى الدول الأعضاء في الإيكاو وقطاع الطيران كوسيلة لمساعدتها على إدارة مخاطر الأمن الإلكتروني في مجال الطيران المدني من خلال اعتماد نهج شامل منسق وكامل.

٢-٢-٢ ينبغي للدول والقطاع والجهات المعنية الأخرى أن تنفذ التدابير الناشئة عن خطة العمل هذه.

الفصل الثالث

خطة العمل الاستراتيجية

٤-١ الركائز السبع لاستراتيجية الأمن الإلكتروني في مجال الطيران

٤-١-١ تم إعداد العناصر الموثقة في هذا الفصل من أجل اقتراح سلسلة من المبادئ والتدابير والإجراءات لتحقيق أهداف الركائز السبع لاستراتيجية الأمن الإلكتروني في مجال الطيران، وهي على الشكل التالي:

١- التعاون الدولي
٢- أساليب الإدارة
٣- التشريعات والتنظيمات الفعالة
٤- سياسة الأمن الإلكتروني
٥- تبادل المعلومات
٦- إدارة الوقائع والتخطيط لحالات الطوارئ
٧- بناء القدرات والتدريب وثقافة الأمن الإلكتروني

الركيزة الأولى: التعاون الدولي
• تطوير التعاون على المستويات الوطنية والإقليمية والدولية بين جميع الأطراف المعنية. • الاعتراف المتبادل بالجهود المبذولة لحماية الطيران المدني (تطوير الأمن الإلكتروني وصيانته وتحسينه). • متابعة تحقيق الاتساق التنظيمي على المستويات العالمية والإقليمية والوطنية بهدف تعزيز الترابط العالمي وضمان القابلية للتشغيل المتبادل لتدابير الحماية. • إشراك الدول في معالجة الأمن الإلكتروني في مجال الطيران المدني الدولي. • تسهيل الفعاليات الدولية في مجال الأمن الإلكتروني والترويج لها. • الإقرار بأن الأمن الإلكتروني مسؤولية مشتركة بين جميع قطاعات منظومة الطيران المدني العالمي.

الركيزة الثانية: أساليب الإدارة
• التشجيع على اعتماد استراتيجيات الإيكاو للأمن الإلكتروني ودعمها والاعتماد عليها. • إعداد المساءلة وأساليب الإدارة على المستوى الوطني للأمن الإلكتروني في مجال الطيران المدني. • ضمان التنسيق على المستوى الوطني فيما بين سلطات الطيران المدني والسلطات الوطنية المختصة في مجال الأمن الإلكتروني. • إنشاء قنوات التنسيق المناسبة فيما بين السلطات الوطنية المتعددة وقطاع الطيران. • تضمين الأمن الإلكتروني في البرامج الوطنية للسلامة ولأمن الطيران المدني. • إدراج الأمن الإلكتروني في الخطط العالمية والإقليمية. • العمل على اعتماد خطة أساسية مشتركة للقواعد والتوصيات الدولية في مجال الأمن الإلكتروني.

الركيزة الثالثة: التشريعات والتنظيمات الفعالة
• ضمان أن تنص المواثيق القانونية الدولية على أطر ملائمة من أجل ردع الوقائع الإلكترونية فضلاً عن محاكمة مرتكبيها. • تحليل التشريعات الوطنية القائمة وتحديث أو اعتماد الملائم منها حسب الضرورة للسماح بردع الهجمات الإلكترونية التي تؤثر في سلامة الطيران المدني أو أمنه أو كفاءته أو استمراريته، والتحقيق فيها وملاحة مرتكبيها قضائياً. • ضمان توافر التشريعات واللوائح التنظيمية الوطنية الملائمة في ما يتعلَّق بالأمن الإلكتروني في مجال الطيران المدني. • إعداد إرشادات ملائمة تساعد الدول وقطاع الطيران في تنفيذ الأحكام المرتبطة بالأمن الإلكتروني.

الركيزة الرابعة: سياسة الأمن الإلكتروني
• ضمان أن يشكل الأمن الإلكتروني جزءا من نُظُم أمن وسلامة الطيران المدني، وكذلك من الأطر الشاملة لإدارة المخاطر. • ضمان إمكانية المقارنة بين المنهجيات المتباينة لتقييم المخاطر المُتعلِّقة بأمن الطيران المدني. • إعداد سياسات الأمن الإلكتروني مع مراعاة دورة الحياة الكاملة لنظم الطيران.

الركيزة الخامسة: تبادل المعلومات
• إعداد منصات وآليات مُعترفٌ بها لتبادل المعلومات، أو تحسين وتحديث القائم منها، على أن تكون متسقة مع أحكام الإيكاو الحالية بهدف إذكاء الوعي بالأمن الإلكتروني، مما يسمح بمنع حدوث الأحداث المرتبطة بالأمن الإلكتروني والكشف عنها بصورة مبكرة والتخفيف من آثارها. • التأكد من إبلاغ السلطة المختصة بأي واقعة أو نقطة ضعف إلكترونية قد تمثل خطراً كبيراً على سلامة الطيران و/أو أمنه.

الركيزة السادسة: إدارة الوقائع والتخطيط لحالات الطوارئ
• ضمان توافر الخطط المناسبة والقابلة للتوسع لتوفير استمرارية سلامة عمليات الطيران المدني وأمنها في حالة حدوث وقائع إلكترونية. • ضمان تحديث خطط الطوارئ الحالية من أجل إدراج أحكام خاصة بالتصدِّي للوقائع المُتعلِّقة بالأمن الإلكتروني والتعافي من آثارها، وتنفيذ تمارين منتظمة/دورية لاختبار القدرات على كشف الوقائع الإلكترونية والتصدِّي لها والتعافي من آثارها.

الركيزة السابعة: بناء القدرات والتدريب وثقافة الأمن الإلكتروني
• ضمان توافر المهارات لدى العاملين، على أساس دور كلٍ منهم، في مجال الطيران والأمن الإلكتروني. • تعزيز مستوى الوعي بالأمن الإلكتروني، بما في ذلك الأنشطة المُتعلِّقة بالتأسيس للنظافة الإلكترونية الملائمة. • ضمان إدراج مناهج الأمن الإلكتروني في الطيران ضمن الأطر التعليمية الوطنية على مستوى التطوير المهني، وذلك من أجل ضمان توافر مجموعة شاملة من المعارف حول أمن الطيران وسلامته على نطاق المنظمة، بما في ذلك كوادر الإدارة العليا بها. • تعزيز الابتكار في مجال الأمن الإلكتروني والترويج لإطلاق البحث والتطوير المناسبين. • تضمين الأمن الإلكتروني في استراتيجية الإيكاو للجيل القادم من المهنيين العاملين في مجال الطيران.

الفصل الرابع

التنفيذ والرصد والاستعراض

٤-١ التنفيذ

إن خطة العمل للأمن الإلكتروني موجهة إلى الإيكاو ودولها الأعضاء وقطاع الطيران والجهات المعنية الأخرى. وتشجع كل هيئة على حدة على اعتماد الأهداف على أساس خارطة الطريق (انظر المرفق (أ)) التي تحدد النتائج الأولوية والإجراءات والمهام ذات الصلة. وذلك من شأنه أن يساعدة الإيكاو والدول والجهات المعنية في التركيز في أعمالها على تنفيذ التدابير والإجراءات الفعالة من أجل بلوغ هدف تطوير إطار عالمي صلب للأمن الإلكتروني في مجال الطيران.

٤-٢ الرصد والاستعراض

ستقوم الإيكاو بإجراء استعراض لخطة العمل، عندما يقتضي الأمر. وستقدم الإيكاو أيضا تحديثا للأهداف والآجال الزمنية، كما تم تحديدها في الخطة. وستشمل هذه التحديثات المجالات حيث تحتاج الدول للمساعدة في تنفيذها لخطة العمل وحيث من الضروري تقديم المساعدة في مجال بناء القدرات وبذل الجهود الأخرى ذات الصلة.

٤-٣ العمل في إطار الشراكات

من الضروري لجميع الجهات المعنية وفي مجال الطيران أن تشارك في هذا الجهد بغية مواصلة تحسين الأمن الإلكتروني في مجال الطيران المدني. وتتيح خطة العمل إطارا مشتركا مرجعيا لجميع الجهات المعنية وتحدد الإجراءات التي ينبغي للإيكاو والدول الأعضاء والصناعة أن تتخذها من أجل تطوير إطار مشترك للأمن الإلكتروني.

٤-٤ دور الإيكاو والدول والجهات المعنية

٤-٤-١ ستضطلع الإيكاو بدور ريادي هام ودور على الصعيد العالمي إلى جانب رصدها لتنفيذ وتنسيق الخطة، بما في ذلك ما يلي:

- تحديث خطة عمل الأمن الإلكتروني، عند الاقتضاء؛
- تطوير القواعد والتوصيات الدولية وإجراءات خدمات الملاحة الجوية وتحديثها، إلى جانب الأدلة والإرشادات الأخرى؛
- رصد واستعراض الحالة فيما يخص المخاطر والتهديدات في مجال الأمن الإلكتروني؛
- تنفيذ المساعدة المحددة لمعالجة الثغرات في الأمن الإلكتروني في مجال الطيران المدني.

٤-٤-٢ تضطلع الدول مع القطاع بدور مهم في تنفيذ خطة العمل للأمن الإلكتروني وتأمين فعاليتها. وتشجع الدول والجهات المعنية على إظهار بشكل سنوي التحسن المسجل في تنفيذ هذه الخطة.

الفصل الخامس

التعاون الدولي

٥-١ إعداد حصر لمبادرات الأمن الإلكتروني في الطيران

٥-١-١ سيتم حصر المبادرات في مجال الأمن الإلكتروني وتحديثها وتوفيرها على بوابة الإيكاو كي تضطلع عليها الجهات المختصة. يتضمن هذا الحصر المبادرات الجارية حاليا، وتشتمل على المبادرات الحالية في مجال الطيران المرتبطة بالأمن الإلكتروني على المستويات العالمي والإقليمية والوطنية. لن يغطي الحصر فقط مبادرات الأمن الإلكتروني في مجال الطيران بل أيضا تلك التي تكون نتائجها مرتبطة بالطيران المدني (مثلا الأمن الإلكتروني في ميادين النقل أو القطاعات الأخرى، مثل الطاقة والمالية).

٥-٢ إعداد الأرضية المشتركة للتشغيل البيني لتدابير الأمن الإلكتروني ونظم الإدارة[٢]

٥-٢-١ ينبغي للدول والقطاع وضع المبادئ والنظم والأدوات المناسبة بهدف ضمان الإدارة الموحدة والآمنة والقابلة للتشغيل البيني المتبادل لنظم الاتصالات وتكنولوجيا المعلومات.

٥-٢-٢ وبما أن الثقة هي الأساس لنظم إدارة فعَّالة وموحدة وقابلة للتشغيل البيني المتبادل من أجل تبادل المعلومات، ينبغي دعم وضع الإطار الثقة للطيران الدولي الذي يسهِّل إدارة المعلومات والقابلية التشغيل المتبادل؛ وعلاوة على ذلك، ينبغي لجميع أصحاب المصلحة المعنيين تحسين السياسات والإجراءات إلى أقصى حد ممكن.

٥-٢-٣ يمكن تحقيق التشغيل البيني لتدابير وإدارة الأمن الإلكتروني من خلال المشاركة في أشكال متعددة لاتفاقات التعاون الدولي. كما ينبغي إنشاء نموذج لمثل هذه الاتفاقات من أجل إتاحة سبل التعاون مع الاستمرار في احترام سياسات الخصوصية وأمن المعلومات والسياسات الأمنية الوطنية المعمول بها. وفي هذا الإطار، يجب تحديد الجوانب التالية كأساس لنماذج الاتفاقات:

- الموضوع وغرض الاتفاقية؛
- الهيئات التي يمكن أن تشارك في مثل هذه الاتفاقات؛
- الأدوار والمسؤوليات المُسندة إلى هذه الهيئات؛
- التدابير التي يمكن استخدامها لتحسين الأمن الإلكتروني في مجال الطيران المدني والتي تخضع للتنسيق.

٥-٢-٤ ينبغي للاتفاقات الدولية أن تحقق ما يلي:

- إنشاء الحوار فيما بين الجهات المعنية لمناقشة الوسائل الهادفة إلى الحد من المخاطر المشتركة وحماية البنية الأساسية للطيران المدني على المستويات الوطنية والدولية؛
- تنفيذ تدابير الحد من المخاطر والتخفيف من حدتها لمعالجة تهديدات الأمن الإلكتروني في مجال الطيران المدني؛
- تبادل المعلومات بشأن التشريعات الوطنية للطيران المدني والاستراتيجيات الوطنية والسياسات وأفضل ممارسات في هذا السياق تتعلق بالأمن الإلكتروني؛

[٢] تتضمَّن نُظُم الإدارة في هذا الإطار، على سبيل المثال لا الحصر، نظم إدارة المخاطر.

- تطوير تدابير لدعم بناء القدرة في مجال الأمن الإلكتروني أينما تقتضي الحاجة.

٥-٢-٥ في إطار يتداخل فيه العديد من المبادئ والنماذج المنهجية إضافة إلى ظهور مصطلحات مختلفة فيما بين الجهات المعنية في مجال الطيران، من الضروري بمكان إعداد معجم مشترك وإطار فهم موحد، لا سيما في ما يتعلَّق بالأمن الإلكتروني في مجال الطيران المدني. وفي هذا السياق، يجب على الإيكاو أن تعد مجموعة عامة من المبادئ بشأن الإدارة المناسبة والعالمية والمتسقة لمخاطر الأمن الإلكتروني، وذلك بالتعاون الوثيق مع الدول الأعضاء والصناعة. وسيتم تحليل الإطار الحالي بهدف تحديد الوسيلة الأفضل لتحقيق التوفيق السلس والفعال بين هذه المبادئ والنماذج.

٥-٣ إعداد المصطلحات المشتركة

٥-٣-١ سيتم برعاية الإيكاو إعداد مصطلحات مشتركة مرتبطة بعبارات الأمن الإلكتروني في مجال الطيران المدني مع مراعاة المصطلحات الحالية المرتبطة بالأمن الإلكتروني ومصطلحات الطيران والأطر ذات الصلة من أجل السماح لجميع الجهات المعنية في مجال الطيران، مهما كانت خلفياتها ومستوى نشاطاتها، أن تفهم وتتفاهم.

٥-٣-٢ يكمن الهدف في تسهيل النشاطات المرتبطة بالأمن الإلكتروني. ولا يعني ذلك أن يتم تحديد و/أو الاتفاق على تعريف واحد لجميع المصطلحات. فمن المقبول أن تظهر تعاريف متعددة لنفس المصطلح (مثلا الاحتمال والشدة والوقوع، إلخ) شريطة أن تكون محددة السياق بحيث لا يؤدي هذا التكرار إلى خلط من شأنه أن يسبب عدم كفاءة في إدارة مخاطر الأمن الإلكتروني في مجال الطيران المدني. وعلى وجه الخصوص، ومع زيادة التركيز على التكامل في إدارة المخاطر في مجال السلامة والأمن، يجب على الإيكاو أن تولي رعاية خاصة لضمان الاتساق بين المصطلحات بشكل سليم. وبالتذكير ببيان السياق الأول المذكور أعلاه، وإضافة إلى التمييز فيما بين الأمن في إطار إدارة الأفعال المقصودة والتدخل غير المشروع والسلامة المرتبطة بمخاطر مقصودة وغير مقصودة وعشوائية، لابد من صقل هذه النواحي لاسيما فيما يتعلق بمسائل الإدارة المتكاملة للمخاطر التي يمكن أن تغطي شواغل الأمن والسلامة على حد سواء (يمكن استخدام الأحكام الواردة في الملحقين السابع عشر والتاسع عشر بمثابة خط أساس في هذا الصدد). وتحديداً، نظراً للتباين بين بؤرة اهتمام كل من السلامة والأمن كمجالين منفصلين (حيث تُعنى السلامة بالمخاطر المقصودة وغير المقصودة والعشوائية، فيما ينصب التركيز في مجال الأمن على الأفعال غير المشروعة والمقصودة)، فإن استحداث أسلوب متكامل في إدارة المخاطر يراعي اعتبارات المجالين معاً مسألة تستلزم الوضوح في تحديد النطاق والغرض من المصطلحات.

٥-٤ تطوير خارطة عامة لتبادل المعلومات والتفاعل في مجال الطيران

٥-٤-١ ينبغي اعتبار توافر إطار موحد لتحديد الخرائط الوظائفية الرفيعة المستوى التي تصف تبادل المعلومات بين جميع الهيئات الفاعلة في مجال الطيران من الشروط المسبقة الضرورية لضمان فهم ساحة المخاطر الإلكترونية بشكل عام. وثمة حاجة لتوافر إطار مشترك غرضه تحديد الخرائط رفيعة المستوى لتبادل المعلومات بين جميع الجهات المعنية في مجال الطيران، وذلك من أجل تحقيق فهم للمخاطر الإلكترونية بشكل عام.

٥-٤-٢ ينبغي لهذه الخارطة الرفيعة المستوى لتبادل المعلومات والتفاعل أن تكون عامة بالقدر الكافي لتشتمل على جميع فئات العمليات المُتعلِّقة بمجال الطيران، وكما ينبغي لها أن تكون، قدر الإمكان، مستقلة عن الهياكل المادية و/أو الفنية المنفذة (نهج الوظائف والخدمات). وينبغي للخارطة الرفيعة المستوى أن تغطي، على سبيل المثال، تدفق البيانات الرقمية لإدارة الحركة الجوية والنشاطات المرتبطة بالمطارات وتدفق البيانات الرقمية للطائرات في عمليات الرحلات الجوية والصيانة. وينبغي لهذه الخارطة أيضا أن تنسق فيما بين أي جهود بدأت بتنفيذها مجموعات أخرى. والغرض من ذلك هو السماح لكل جهة من الجهات المعنية أن تستكمل خارطة خاصة بها أو تكيفها أو تغيرها حسب احتياجاتها فيما يخص سبل التفاعل مع الجهات الأخرى. وفي نهاية المطاف، ينبغي على كل جهة من الجهات المعنية أن تكون قادرة على تطوير أو تكييف هذه الخارطة بحسب حالتها الخاصة. ووفقاً لذلك،

فإن نتائج عمليات تقييم المخاطر الأمنية التي تقوم بها أي من الجهات باستخدام منهجيتها ومعاييرها الخاصة (التي يمكن أن تكون قابلة للمقارنة على أساس إطار مشترك لتقييم المخاطر – انظر الفقرة ٥-٦) يمكن تبادلها وتقاسمها مع الجهات المعنية الأخرى بالقدر الممكن. وبالعمل سويا، وباستخدام الأطر القابلة للمقارنة لتقييم مخاطر الأمن وبالاعتماد على خارطة تبادل المعلومات والتفاعل، ستتمكن الجهات المعنية من فهم كيف تنتشر المخاطر أو كيف يمكن لشركاء آخرين أن يديروا هذه المخاطر وبالتالي يتم السماح بتبادل المعلومات بشأن المخاطر التي تتعرض لها إحدى الجهات المعنية أو تنشأ عنها.

٥-٥ تطوير تبادل المعلومات عن المخاطر فيما بين المنظمات

٥-٥-١ ثمة العديد من القواعد القياسية والوثائق الإرشادية التي تتناول مسؤولية كل منظمة على حدة فيما يخص إدارة الأمن الإلكتروني لديها، وأي عند معالجة النظم والإجراءات والمنتجات والبيانات الداخلية. ولكن بما أن مخاطر الأمن الإلكتروني المتربصة بالطيران المدني تُعد مخاطر مشتركة بين عدد من الجهات المعنية، فثمة حاجة إلى النظر إلى ما هو أبعد من فرادى المنظمات. ولتحقيق الإدارة الفعالة والكفء للمخاطر المشتركة، يجب التأكيد على تشاطر المعلومات عن المخاطر المترسخة في ظروف عمل حيث تكون النظم أو الإجراءات أو المنتجات أو البيانات متقاسمة مع منظمات أخرى أو منقولة من منظمة إلى أخرى.

٥-٥-٢ ينبغي النظر في إبرام اتفاقات خارجية مع موردين خارجيين لتمكين المنظمة والسلطات/الجهات التنظيمية المعنية من تبادل المعلومات الحساسة المتعلقة بالأمن الإلكتروني فيما بينها من أجل تسهيل إدارة مخاطر والتهديدات المُتعلِّقة بسلسلة التوريد.

٥-٦ تحديد المعايير لإمكانية مقارنة تقييم المخاطر

٥-٦-١ في سياق المخاطر التي تشمل أكثر من منظمة، من الضروري أن تفهم الجهات المعنية المخاطر الشاملة، وما يتصل بذلك من مدى إقبال الأطراف المعنية الأخرى على المخاطر من أجل إدارتها. وفي هذا السياق، ينبغي تطوير الفهم الميسّر لتقييم مخاطر الأمن الإلكتروني وقابليتها للمقارنة.

٥-٧ تطوير التنسيق المناسب فيما بين السلطات المدنية والعسكرية

٥-٧-١ ينبغي أن تنشئ سلطات الطيران المدني والسلطات العسكرية المختصة القدرات والخطوات المناسبة للتعاون بشأن المسائل المُتعلِّقة بالأمن الإلكتروني، حيثما أمكن، وبشكل متسق مع القانون الوطني، ويشمل ذلك على سبيل المثال لا الحصر شروط الأمن القومي والدفاع الوطني.

٥-٧-٢ إن تبادل المعلومات المرتبطة بالأمن الإلكتروني والتنسيق المناسب بين الجهات المعنية العسكرية والمدنية في مجال الطيران منذ المراحل الأولى يمكن أن يعودا بالمنافع الجمة في تحديد التهديدات والمخاطر الإلكترونية المحتملة، ما من شأنه أن يساهم في النجاح في التخفيف من حدة المخاطر الإلكترونية المتربصة بالطيران في منظومة الطيران.

٥-٧-٣ يكتسب تبادل المعلومات بين الجهات المعنية المدنية والعسكرية في مجال الطيران أهمية في إدارة الأزمات المرتبطة بالأمن الإلكتروني. ويمكن أن تقدم الدول دعمها للجهات المعنية المدنية والعسكرية لديها في مجال الطيران في تنظيم الترتيبات التي من شأنها أن تسهل تبادل المعلومات من خلال الآليات المناسبة، بالقدر المستطاع من الناحية العملية.

٥-٨ الترويج للفعاليات العالمية والإقليمية بشأن الأمن الإلكتروني في مجال الطيران المدني

٥-٨-١ ستدعم الإيكاو وتنظم الفعاليات العالمية والإقليمية للترويج للأمن الإلكتروني في مجال الطيران المدني، حسب الاقتضاء.

الفصل السادس

أساليب الإدارة

٦-١ إنشاء هيكل لأساليب الإدارة

٦-١-١ يتعين على الإيكاو أن تنشئ هيكلاً داخلياً لأساليب الإدارة من أجل الأمن الإلكتروني في مجال الطيران بحيث يضمن اتباع نهج كلي شامل قائم على المخاطر في ما يتعلَّق بالأمن الإلكتروني والقدرة على الصمود في وجه التهديدات والهجمات الإلكترونية على مستوى جميع مجالات الطيران والخبرات ذات الصلة.

٦-١-٢ وبالإضافة إلى ذلك، ينبغي للدول أن تُحدِّد وتنفذ هياكل وطنية للإدارة والمساءلة في ما يتعلق بالأمن الإلكتروني في مجال الطيران المدني، بما يكفل تطوير وتنفيذ متطلبات الأمن الإلكتروني والقدرة على الصمود في وجه التهديدات والهجمات الإلكترونية على الصعيدين الوطني والدولي، فضلاً عن تحديد أدوار ومسؤوليات كل طرف من الأطراف المعنية على الصعيد الوطني. وينبغي أيضاً أن يأخذ هذا التطوير في الاعتبار التنسيق المطلوب بين السلطات الوطنية المختصة في مجال الطيران المدني والأمن الإلكتروني.

٦-٢ إعداد خطة (خطط) للأمن الإلكتروني تمتد لعدة سنوات

٦-٢-١ يُوصى بأن تكون خطة عمل الأمن الإلكتروني متسقة بصورة ملائمة مع الخطة العالمية لأمن الطيران (GASeP) والخطة العالمية للملاحة الجوية (GANP) والخطة العالمية لسلامة الطيران (GASP)، كما ينبغي تضمين هذه الخطط الجوانب الخاص بالأمن الإلكتروني، حسب الاقتضاء.

٦-٢-٢ من أجل ضمان تنفيذ وتطبيق الخطط العالمية بشكل سليم على الصعيد الوطني، فإن الدول مدعوة إلى إدراج الإجراءات المُنسَّقة والمناظرة ذات الصلة بالأمن الإلكتروني على الصعيد الوطني في برامجها الوطنية للسلامة والأمن، وفي خططها للملاحة الجوية.

٦-٣ تطوير أساليب الإدارة والمساءلة

٦-٣-١ ينبغي للإيكاو أن تطور مواد إرشاديةً تتعلق بسياسة الأمن الإلكتروني من أجل تسهيل التناغم والاتساق فيما بين سياسات الأمن الإلكتروني العالمية والإقليمية والوطنية.

٦-٣-٢ يجب أن تكون أساليب الإدارة في مجال الأمن الإلكتروني قائمة على السياسات وتنفيذها، ولابد من تحديد أوجه المساءلة لأغراض الامتثال.

٦-٣-٣ ينبغي أن تتخذ الدول التدابير الملموسة للاستمرار في تحسين فعالية إجراءات إدارة الأمن الإلكتروني وجودتها واتساقها على المستوى الوطني.

٦-٣-٤ إذا كان هناك ما يبرر ذلك، يمكن أن تكون نظم إدارة أمن المعلومات (ISMS) أدوات فعَّالة في إدارة الأمن الإلكتروني، ويمكن تنفيذها على مستوى الدولة أو المنظمة[٣].

[٣] عند تطوير الإدارة للأمن الإلكتروني على المستوى الوطني، يجوز للدول أن تسترشد بالمعيار ISO 27001 لتحديد مبادئ الريادة، مثل ضمان إدماج شروط نظام إدارة أمن المعلومات في العمليات التنظيمية وضمان توافر الموارد اللازمة وضمان تحقيق نظم إدارة أمن المعلومات للنتائج المرجوة منها.

الفصل السابع

الأطر التشريعية والتنظيمية الفعَّالة

٧-١ استعراض المواثيق الدولية الحالية في مجال قوانين الجو الدولية وعلاقتها بالأمن الإلكتروني

٧-١-١ ستقوم الإيكاو بتحليل مواثيق قوانين الجو الدولية الحالية لتحديد الثغرات القائمة والمحتملة في ما يتعلق بالمخاطر الإلكترونية. وستقترح الإيكاو الحلول الممكنة لسد الثغرات التي تم تحديدها، إن وجدت، بهدف تعزيز حماية الطيران المدني.

٧-٢ ضمان اتساق أحكام الإيكاو مع حاجات الأمن الإلكتروني

٧-٢-١ مع تطور مسألة الأمن الإلكتروني في مجال الطيران المدني، قد تكون هناك حاجة إلى تطوير الأحكام من أجل أن تتمّم القواعد والتوصيات الدولية وإجراءات خدمات الملاحة الجوية الحالية أو تضيف إليها. وينبغي القيام بذلك التطوير بأخذ كل حالة على حدة، مع الإشارة إلى أنه ينبغي تفادي إضافة أحكام جديدة خاصة بالقواعد والتوصيات الدولية وإجراءات خدمات الملاحة الجوية إلى الحد الأقصى المستطاع أو ينبغي أن يتم تنسيقها، عند الضرورة، فيما بين جميع الأطراف المعنية.

٧-٣ التصديق على اتفاقية وبروتوكول بيجين

٧-٣-١ الدول مدعوة إلى التصديق على *اتفاقية قمع الأفعال غير المشروعة المتعلقة بالطيران المدني الدولي* (اتفاقية بيجين لعام ٢٠١٠) *والبروتوكول المكمل لاتفاقية قمع الاستيلاء غير المشروع على الطائرات* (بروتوكول بيجين لعام ٢٠١٠).

٧-٤ ضمان الدول وضع التشريعات والتنظيمات المناسبة وتطبيقها على المستوى الوطني

٧-٤-١ الدول مدعوة إلى تقييم ما لديها من أطر قانونية وطنية في مجال الأمن الإلكتروني والطيران المدني بهدف تحديد الثغرات الحالية ، وأيضاً لضمان توافر التشريعات واللوائح التنظيمية المناسبة لمعالجة عناصر محددة في الأمن الإلكتروني في مجال الطيران المدني. ويظهر عنصر رئيسي آخر في توافر آلية الإنفاذ التي تشجع الدول على تفعيلها، إن لم تكن موجودة بالفعل في أطرها القانونية الوطنية، لتجريم ومقاضاة الأفعال غير المشروعة ضد الطيران المدني عند ارتكابها باستخدام وسائل إلكترونية.

الفصل الثامن

سياسة الأمن الإلكتروني

٨-١ وضع سياسات الأمن الإلكتروني وتطبيقها

٨-١-٢ ينبغي وضع سياسة للأمن الإلكتروني على الصعيدين الوطني والمؤسسي. وينبغي أن يكون لدى الدول سياسة واضحة وفعَّالة في مجال الأمن الإلكتروني، بما في ذلك:

- الأهداف المنبثقة عن نتائج عمليات تقييم مخاطر الأمن الإلكتروني في مجال الطيران المدني؛
- الالتزام بالوفاء بالمتطلبات المعمول بها وطريقة تقييم الامتثال؛
- الاعتبارات المتعلقة بالإدارة والتنسيق مع الجهات الخارجية التابعة (انظر الفصل بشأن التعاون الدولي)؛
- الالتزام بالتحسين المستمر لإطار الأمن الإلكتروني؛
- الأحكام التي تضمن بأن تكون السياسة موثقة بصورة كاملة ومتاحة كمعلومات رسمية؛
- الأحكام التي تضمن نشر السياسة على النحو الملائم.

٨-٢ تحديد وتقييم المخاطر الإلكترونية المحدقة بالطيران المدني

٨-٢-١ يتمثل أحد التحديات في إطار أنشطة تحديد المخاطر وتقييمها في القدرة على توقع التغيرات السريعة التي تطرأ على منابع التهديدات وخصائصها. ويُعتبر توقع التهديدات المتغيرة أساسيا لمساعدة منظومة النقل الجوي على تكييف استراتيجية الحماية الخاصة بها على نحو استباقي ليس فقط وفقًا للتهديدات الحالية، ولكن أيضًا في ضوء التهديدات المحتملة مستقبلا. وبفضل هذا التوقع، ينبغي أن يكون قطاع الطيران المدني قادراً على التمتّع بقدرٍ أكبر من الاستباقية في سياق يكون فيه تباين بين مرونة المهاجمين شديدي المرونة والتكيف والمدافعين البطيئين في ردّ الفعل، بالنظر إلى تعقيد النظام الذي ينبغي حمايته. ففي هذا السيناريو، يصبح هذا النهج الاستباقي أكثر أهمية، فمن الضروري إنشاء إطار لتحديد وتقييم مخاطر الأمن الإلكتروني يدعم هذه الحاجة من أجل المساعدة في التخفيف من هذه المخاطر.

٨-٢-٢ ويوصى بتحديد وتقييم مخاطر الأمن الإلكتروني مع مراعاة جميع العواقب المحتملة لأيّ هجوم على منظومة الطيران المدني (الأمن والسلامة والكفاءة والقدرة على الصمود واستمرارية الخدمة، وما إلى ذلك). وكذلك جميع مصادر التهديد المحتملة ونقاط الضعف القائمة أمام هذه التهديدات. وينبغي أن يستند هذا النشاط إلى مصفوفات المخاطر الإلكترونية التي تمّ إعدادها مسبقًا تحت رعاية مجموعة عمل التهديدات والمخاطر التابعة لفريق خبراء أمن الطيران (WGTR).

٨-٢-٣ وبما أنّ نسبة كبيرة من المخاطر المحدقة بالأمن الإلكتروني للطيران المدني مشتركة بين العديد من الجهات المعنية، يوصى بالنظر في خرائط تبادل المعلومات/التفاعل في مجال الطيران (انظر الفصل ٦-١). وينبغي استخدام تلك الخرائط كوسيلة لضمان شمولية السيناريوهات التي يتم النظر فيها والسماح للجهات المعنية فهم طريقة تفاعلها مع بعضها البعض واعتمادها على المخاطر.

٨-٢-٤ وبما أنّ مستوى شدة المخاطر في مجال الأمن الإلكتروني سيتغير بمرور الوقت، كما أنه يمكن لهذه المخاطر أن تتطور بسرعة مقارنةً بالمخاطر الأخرى، يوصى بالنظر في وسيلة لتعديل أي استجابة لهذه المخاطر المحدقة بالطيران عالمياً بما يمكن نشرها بشكل سريع ومتسق (مثل الموازنة بين الحاجة إلى القواعد القياسية للطيران والمواد الإرشادية وأفضل الممارسات المتبعة خارج قطاع الطيران، واستخدام/الاعتماد على الاستجابات المطبقة في المجالات الأخرى) .

٨-٢-٥ ويوصى بإسناد تنفيذ وتنسيق عمليات تحديد وتقييم مخاطر الأمن الإلكتروني إلى مجموعة من الخبراء مكوّنة من خبراء في الأمن الإلكتروني في مجال الطيران المدني، أو، إذا تعذر ذلك، يمكن الاستعانة بفريق من الخبراء في الأمن الإلكتروني وفي الطيران المدني، ويفضل تمتع أعضاء الفريق بخلفية واسعة في الأمن الإلكتروني.

٨-٢-٦ وينبغي لمجموعة الخبراء هذه أن تكون مسؤولة عن وضع "بيان سياق المخاطر العالمية في مجال الأمن الإلكتروني".

الفصل التاسع

تبادل المعلومات

يُعتبر تبادل المعلومات ذات الصلة بالأمن الإلكتروني مسألة هامة لإدارة مخاطر الأمن الإلكتروني على نُظُم الطيران المدني. واعترافاً بأنّ الترويج لتبادل المعلومات يُعتبر عنصراً رئيسياً في إنشاء ثقافة الأمن الإلكتروني، ينبغي للجهات المعنية في مجال الطيران المدني أن تقوم بإعداد وتنفيذ، أو تحديث القائم من، البرامج التي تتيح إمكانية تبادل المعلومات ضمن منظماتها أو مع الأطراف الخارجية، بقدر ما هو ممكن. ومن خلال هذه البرامج، ينبغي أن تبرم الجهات المعنية شراكات وتتبادل المعلومات الجوهرية مع الجهات المعنية الأخرى التي تمتلك وتشغل البنية الأساسية للطيران المدني، إلى جانب ضرورة إعداد خطط وممارسات لتبادل المعلومات ضمن منظماتها.

وينبغي أن تتيح برامج تبادل المعلومات الفرصة أمام تطوير وتشغيل وتعديل أساليب الدفاع الإلكترونية عن الطيران المدني في وجه التهديدات الإلكترونية المعروفة والناشئة، كما ينبغي أن تساعد تلك البرامج على تطوير ما يلي:

- الوعي بالأوضاع في أثناء العمليات اليومية الاعتيادية وخلال الأزمات أو الوقائع أو الأحداث؛
- الإدارة التشغيلية والتكتيكية للمخاطر توقعا لوقوع تهديد ما أو استجابةً له؛
- التخطيط الاستراتيجي لبناء القدرات التي من شأنها تعزيز الأمن الإلكتروني والمرونة في وجه المخاطر مستقبلاً.

٩-١ تطوير تبادل المعلومات عن المخاطر

٩-١-١ تبادل المعلومات المتعلقة بالأمن الإلكتروني له أبعاد ثنائية ومتعددة الأطراف – أي مزيج بين وعبر (على المستوى الوطني والإقليمي والعالمي) الأطراف التالية:

- سلطات الأمن الإلكتروني الوطنية؛
- سلطات الطيران المدني الوطنية؛
- سلطات الطيران العسكري الوطنية؛
- الجهات المعنية الأخرى في مجال الطيران (المشغلون ومقدمو الخدمات والمصنعون)؛
- الجهات المعنية العاملة خارج مجال الطيران (مقدمو خدمات تكنولوجيا المعلومات والاتصالات فضلا عن سلسلة الإمدادات).

٩-١-٢ ومن المعترف به أن هناك العديد من أنواع المعلومات المتعلقة بالأمن الإلكتروني، مثل:

- *المعلومات الاستخباراتية الإلكترونية* – مثل المشهد العام للتهديدات والمعلومات الاستخبارية بشأن قدرات ونوايا الجهات الفاعلة في مجال التهديدات الإلكترونية.
- *مؤشرات التعرّض للاختراق (IoCs)*.
- *التكتيكات والتقنيات والإجراءات (TTPs)*، مثل سيناريوهات الهجمات والأساليب التي يُفضِّل المتسللون استخدامها.
- *نقاط الضعف*، مثل الأجهزة والبرمجيات والخدمة والبروتوكول والمعيار، وما إلى ذلك، بما في ذلك سيناريوهات الاستغلال المحتملة.
- *تقارير الوقائع*.

٩-١-٣ ورهناً بالتشريعات الوطنية وبطبيعة المعلومات المتعلقة بالأمن الإلكتروني، قد تكون هناك منهجيات وقيود مختلفة لتشاطر المعلومات مع مختلف المتلقين (مثل السلطة الوطنية المعنية بالأمن الإلكتروني والسلطة الوطنية للطيران المدني والسلطة الوطنية للطيران العسكري وغيرها من الجهات المعنية في مجال الطيران).

٩-١-٤ ينبغي تحديد تبادل المعلومات واحتياجات التعاون (بما في ذلك على سبيل المثال لا الحصر في أوقات الأزمات) والسياسات على المستوى العالمي والإقليمي والوطني.

٩-١-٥ يوصى باستخدام بروتوكول إشارات المرور (TLP)[٤] لتحديد مستوى التوزيع/التقييد عند توزيع ومواصلة تشاطر المعلومات المتعلقة بالأمن الإلكتروني.

٩-١-٦ بقدر ما هو ممكن، ينبغي إلغاء تحديد الهويّة في المعلومات ذات الصلة بالأمن الإلكتروني والتي قد تتضمّن معلومات حساسة أو تعقيمها قبل تبادلها، بدلاً من عدم تبادلها على الإطلاق.

٩-٢ وضع مبادئ وإرشادات من الأجل الإفصاح المسؤول من جانب الباحثين في مجال الأمن

٩-٢-١ نظراً لتنامي اهتمام مجتمع الباحثين في مجال الأمن بالأمن الإلكتروني للطيران المدني، ولتجنب الإفصاح غير المسؤول عن النتائج المحتملة الذي قد يضرّ بأمن وسلامة الطيران المدني ويضر أيضاً بكفاءته واستمراريته، يجب تحديد مبادئ الإفصاح المسؤول عن مواطن الضعف التي اكتشفها الباحثون الأمنيون، أو الأطراف الثالثة من أجل ضمان أنّ مبادئ الإفصاح ليست مؤذية للأمن الإلكتروني في مجال الطيران المدني. وينبغي أن يأخذ ذلك في الاعتبار التوصية ٤-٤ في استراتيجية الأمن الإلكتروني.

٩-٢-٢ ينبغي وضع إرشادات لهذه المبادئ (تتناول على سبيل المثال، ضمن جملة شواغل أخرى، الاكتشاف وإخطار الصانعين والتحقيق والمعالجة وإخطار قطاع الطيران والمعالجة وأخيراً النشر العلني) بين الباحثين والأطراف الثالثة، من جهة، وسلطات الطيران والجهات المعنية في مجال الطيران، من جهة أخرى، لضمان عدم تأثير أنشطة البحث، إلى أقصى حد ممكن، عن/اكتشاف مواطن الضعف هذه والإفصاح عنها على السلامة وتوفير الخدمات. وفي أفضل الظروف، لن تتناول الإرشادات عمليات الإفصاح المسؤولة فحسب، بل تشمل أيضًا عناصر التوعية والتثقيف.

٩-٣ إنشاء شبكة عالمية من سلطات الأمن الإلكتروني الإقليمية/الوطنية لأغراض الطيران المدني

٩-٣-١ لم يتم تحديد المسؤولية عن الأمن الإلكتروني داخل الدول والقطاع بشكل موحد، والخبرة المناسبة موزّعة عبر مجموعة واسعة من الجهات المعنية من داخل قطاع الطيران وخارجه والمجالات الوظائفية. والبديهي أن يؤدي هذا التنوع إلى صعوبة في تحديد جهة الاتصال المناسبة داخل أي هيئة من الهيئات، فضلاً عن صعوبة إنشاء وتحديث قنوات اتصال رسمية بين الجهات المعنية. كذلك فإن الإرشادات المتعلّقة بإنشاء وصيانة جهة اتصال واحدة تختص بالمسائل المتعلقة بالأمن الإلكتروني في مجال الطيران المدني داخل الدول والمؤسسات من شأنها تسهيل إقامة قنوات اتصال عالمية وإقليمية ووطنية وبناء دوائر ملائمة تحتص بالأمن الإلكتروني فضلا عن نشر ثقافة الأمن الإلكتروني.

٩-٤ القدرة العالمية على تبادل معلومات الأمن الإلكتروني لأغراض الطيران

٩-٤-١ يمكن تطوير قدرات تبادل المعلومات على نحو شامل لأغراض الطيران المدني على المستوى العالمي والإقليمي و/أو الوطني لتعزيز تبادل المعلومات المتعلقة بالأمن الإلكتروني.

٩-٤-٢ قد تشمل منتديات تبادل المعلومات بين كيانات عامة وكيانات عامة ، وكيانات عامة وكيانات خاصة ، وكيانات خاصة وكيانات خاصة. وينبغي للأطراف المعنية أن تنخرط في مجتمعات موثوق بها لتسهيل تبادل أفضل الممارسات والاستخبارات المُتعلِّقة بالتهديدات.

---

[٤] يُرجى الرجوع إلى إرشادات الإيكاو المعنونة "إرشادات الإيكاو بشأن بروتوكول إشارات المرور".

الفصل العاشر

إدارة الوقائع والتخطيط لحالات الطوارئ

١٠-١ تطوير قدرات الاستجابة للوقائع والتخطيط للاستجابة لحالات الطوارئ

١٠-١-١ يتعين على جميع الجهات المعنية تطوير آليات الاستجابة للوقائع والطوارئ واختبارها مع شركائها التشغيليين على نحو منسق، ويشمل ذلك ما يلي:

- الاستفادة من خطط الطوارئ الحالية التي تم إعدادها بالفعل و/أو تعديلها لتشمل أحكاماً بشأن الأمن الإلكتروني؛
- قيام الجهات المعنية في الطيران المدني بوضع وتحديث خطط مناسبة قابلة للتعديل بما يضمن الأمن والسلامة والاستمرارية لعمليات النقل الجوي خلال الوقائع الإلكترونية المحتملة؛
- وضع أحكام بشأن الاستجابة لوقائع الأمن الإلكتروني والقدرات على التعافي، بما في ذلك خطط الطوارئ والاستجابة لحالات الطوارئ؛
- إشراك الجهات المعنية في مجال الطيران العسكري بشكل استباقي في عملية التخطيط، لإنشاء خطوط اتصال ؛
- تحقيق مستويات أداء مقبولة وتلبية متطلبات الحفاظ على الحد الأدنى لمستويات الخدمات الأساسية؛
- تطوير فئات متجانسة ومتناغمة من أجل الإبلاغ عن الوقائع الإلكترونية، والتنسيق بين نُظُم الإبلاغ عن الوقائع المتعلِّقة بالأمن الإلكتروني في مجال الطيران المدني على المستويات الوطنية والإقليمية، والدولية أيضاً عند الاقتضاء.
- ينبغي أن يقوم أصحاب المصلحة في مجال الطيران بصورة دورية بإجراء جلسات محاكاة مكتبية وتدريبات حية لاختبار صحة الافتراضات التي روعيت في التخطيط.

١٠-٢ وسائل الكشف عن الوقائع وتحليلها والتصدي لها على مستوى الجهات المعنية

١٠-٢-١ ينبغي تنفيذ خطط التصدي للوقائع إلى الحد الممكن، كما ينبغي على الجهات المعنية تطوير قدرات الكشف عن وقائع الأمن الإلكتروني وتحليلها والتصدي لها على كافة المستويات. ومن المهم رصد حالة الأمن الإلكتروني لتلك النظم/الخدمات حسب الاقتضاء لدعم الطيران المدني، من أجل اكتشاف المشكلات المحتملة وتتبع الفعالية المستمرة لتدابير الحماية الأمنية. وبمجرد اكتشافها، ينبغي تحليل وقائع الأمن الإلكتروني ووضع خطط الاستجابة المناسبة موضع التنفيذ؛ وينبغي أن تشمل هذه الخطط إجراءات تخفيف للحد من تأثير واقعة الأمن الإلكتروني.

١٠-٣ إنشاء خليّة لتنسيق الأزمات من أجل الأمن الإلكتروني في مجال الطيران المدني

١٠-٣-١ متى أمكن، ينبغي إنشاء خلية لتنسيق الأزمات في مجال الطيران المدني تشتمل على خبرة في الأمن الإلكتروني للطيران المدني (بالاستناد إلى الآليات الموجودة بالفعل)، وعند الاقتضاء، ينبغي إشراك الجهات المعنية في مجال الطيران العسكري.

١٠-٣-٢ وينبغي إجراء تمارين دورية على نحو منتظم، لا سيّما جلسات المحاكاة المكتبية بمشاركة جميع الجهات المعنية في المجال عند الاقتضاء.

الفصل الحادي عشر

بناء القدرات والتدريب وثقافة الأمن الإلكتروني ونشر الوعي

١١-١ تطوير القدرات الفنية والتدريب وثقافة الأمن الإلكتروني ومواد التوعية

١١-١-١ ينبغي تعريف عناصر التثقيف والتدريب والوعي بثقافة الأمن الإلكتروني في مجال الطيران المدني والترويج لها على المستوى العالمي والإقليمي والوطني.

١١-١-٢ وينبغي الترويج للأمن الإلكتروني والأنشطة التثقيفية على مستوى الإدارة العليا من خلال منظمات الطيران المدني كما ينبغي تسليط الضوء على الأدوار الأساسية لمختلف الجهات الفاعلة وتوقعاتها. وينبغي أن تؤدي ثقافة الأمن الإلكتروني والتثقيف إلى تطوير قاعدة معارف بشأن الأمن الإلكتروني في مجالي سلامة الطيران وأمن الطيران، بحيث تشمل ما يلي:

- المفاهيم المتعلّقة بمبادئ الأمان بفضل التصميم للتخفيف من حدة التهديدات الإلكترونية، بالتنسيق مع مجتمع السلامة. وينبغي أن تساعد هذه المفاهيم مجتمع السلامة الجوية في اتخاذ قرارات مستنيرة عند معالجة التهديدات الإلكترونية؛
- اتباع نهج منسق فيما بين الجهات المعنية في مجالي الأمن والسلامة، مع الإقرار بأنّ الضوابط الأمنية يجب ألا تؤثر سلبا على سلامة الرحلات، بما يتيح نقل المعرفة الفنية ويضمن اتخاذ القرارات المستنيرة بالاستناد إلى فهم متبادل لساحة المخاطر؛
- مفاهيم ممارسات التحصّن ضد الهجمات الإلكترونية لموظفي التشغيل والدعم والتي ينبغي أن تساعد في تفادي الآثار الضارة المحتملة على منظومة الطيران المدني الناجمة عن العدد المتزايد من "المنتجات التجارية الجاهزة للاستعمال" ((Commercial Off the Shelf" (COTS) والبرمجيات الخبيثة غير المحددة؛
- ومفاهيم "الثقافة العادلة" من جانب مجتمع السلامة لتمكين وتحفيز الإبلاغ الذاتي عن الوقائع الناجمة عن السلوك غير المقصود من قبل الموظفين (مثل الممارسات المهنية السيئة غير المقصودة في استخدام شريحة الذاكرة USB Stick).

١١-١-٣ عند تنفيذ هذه الأنشطة، ينبغي التركيز على التأثير أو التأثير المحتمل.

١١-١-٤ وينبغي أن يساعد تطوير ثقافة الأمن الإلكتروني والترويج لها ولمواد التوعية في إقامة فهم متبادل/مشترك بين مجتمعي السلامة والأمن لساحة المخاطر في مجال الأمن الإلكتروني، بالإضافة إلى تعززي الثقة المتبادلة في التدابير المضادة المعمول بها.

١١-١-٥ ينبغي أن تشجّع الإيكاو برامج التبادل فيما بين الدول والأقاليم بشأن التثقيف والتدريب في مجال الأمن الإلكتروني.[٥]

[٥] كما هو الحال، على سبيل المثال، في ما يتعلّق بمبادرات الحرم الجامعي متعدد الجنسيات أو شبكة ومراكز الاتحاد الأوروبي للكفاءة في مجال الأمن الإلكتروني.

٦-١-١١ وينبغي ألا تقتصر الأنشطة المتعلقة بثقافة الأمن الإلكتروني والتثقيف على تشغيل النظم فقط، بل يجب أن تُعنى أيضاً بدورة حياتها النظام بأكملها، ويشمل ذلك ما يلي:

- الشرط (الأمن جزء متكامل بالفعل في مرحلة المُتطلَّبات)؛
- التصميم (اتباع استراتيجية آمنة حسب التصميم، أمن الأجهزة، والبرمجيات والبيانات، وإدارة التغيير، وإدارة مواطن الضعف)؛
- التطوير (بيئة آمنة، واختبار أمني مستمر ومتكامل)؛
- التصنيع / الاستحواذ (بما في ذلك سلسلة توريد الأجهزة والبرامج الخاصة بتكنولوجيا المعلومات والتقنيات التشغيلية)؛
- التشغيل (إدارة الوصول، سلامة البيانات، تشغيل النظم المأمونة)؛
- الصيانة (بما في ذلك استراتيجيات الإصلاح والتحديث)؛
- التخلص (بما في ذلك إدارة بيانات تسجيل الدخول والبيانات المتبقية على أجهزة التخزين).

الفصل الثاني عشر

الاستنتاج

تجمع خطة عمل الأمن الإلكتروني بين الإيكاو والدول وقطاع الطيران والجهات المعنية الآخرين في إطار جهد متكامل ومنسّق لمواجهة تحديات الأمن الإلكتروني الحالية والناشئة. وهي تسلِّط الضوء على أنّ الأمن الإلكتروني هو مسألة شاملة تشترك فيها جميع مجالات قطاع الطيران. كما أن هذه الخطة تساعد على تنفيذ استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران، والتحرُّك صوب إنشاء إطار عالمي متين للأمن الإلكتروني.

— — — — — — — —

المرفق (أ)

خارطة طريق خطّة عمل الأمن الإلكتروني

الإجراءات العامّة ضمن استراتيجية الأمن الإلكتروني

النتائج ذات الأولويّة	وضع رؤية شاملة متفق عليها
الإجراءات ذات الأولوية	• الإقرار بضرورة إعداد رؤية شاملة ومتفق عليها بشأن الأمن الإلكتروني بحيث تكون الأساس الذي تستند إليه أساليب قوية ومنسقة في إدارة المخاطر في مجال الطيران العالمي؛ • الإقرار بوجوب أن يتمتع قطاع الطيران المدني بالمرونة اللازمة في وجه الهجمات الإلكترونية، وأن يظل آمناً وموثقاً به عالمياً، مع مواصلة الابتكار والتطوّر؛ • الإقرار بأن المخاطر المرتبطة بالأمن الإلكتروني في مجال الطيران تندرج في إطار اتفاقية الطيران المدني الدولي.

الإجراءات					
رقم الإجراء في خطّة العمل	**الجهة المعنية**	**الإجراءات/المهام المحددة**	**المؤشرات**	**الأولوية**	**تاريخ بدء التنفيذ**
CyAP 0.1	الإيكاو والدول الأعضاء وقطاع الطيران	تتولى الإيكاو وضع نموذج لسياسة الأمن الإلكتروني كمرجع للدول الأعضاء وقطاع الطيران عند قيامهم بتطوير سياساتهم الوطنية والمؤسسية.	النموذج متاح للدول الأعضاء والقطاع	مرتفعة	٢٠٢١
CyAP 0.2	الإيكاو والدول الأعضاء	البدء في تنفيذ الأعمال المرتبطة باستراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران على المستوى الوطني (بحسب ما جاء في قرار الجمعية العمومية ٤٠-١٠) (من أجل التحقق من كيفية تنفيذ الدول للاستراتيجية، يجب وضع مجموعة من المقاييس لقياس تنفيذ إجراءات معينة).	دليل وطني على البدء بأعمال التنفيذ	مرتفعة	٢٠٢٣
CyAP 0.3	الإيكاو	إجراء دراسات استقصائية لتحديد كيفية تنفيذ الدول لاستراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران. (دراسة استقصائية للسؤال عما إذا كانت الدول قد وضعت خطة عمل لتنفيذ الاستراتيجية)	دراسة استقصائية/استبيان تعدّه الإيكاو وترسله إلى الدول الأعضاء	مرتفعة	٢٠٢١-٢٠٢٢

ركائز استراتيجية الأمن الإلكتروني

النتائج ذات الأولويّة	١- إقامة التعاون الدولي
الإجراءات ذات الأولوية	• تطوير التعاون على الأصعدة الوطنية والإقليمية والدولية بين جميع الأطراف المعنية. • الاعتراف المتبادل بالجهود المبذولة لحماية الطيران المدني (تطوير الأمن الإلكتروني وصيانته وتحسينه). • متابعة تحقيق الاتساق التنظيمي على المستويات الدولية والإقليمية والوطنية من أجل تعزيز الترابط العالمي وضمان القابلية للتشغيل المتبادل لتدابير الحماية. • إشراك الدول في معالجة الأمن الإلكتروني في مجال الطيران المدني الدولي. • تسهيل الفعاليات الدولية في مجال الأمن الإلكتروني والترويج لها. • الإقرار بأن الأمن الإلكتروني مسؤولية مشتركة بين جميع قطاعات منظومة الطيران المدني العالمي.

الإجراءات

رقم الإجراء في خطّة العمل	الجهة المعنية	الصلة باستراتيجية الأمن الإلكتروني في مجال الطيران	الصلة بالفصل الخامس	الإجراءات/المهام المحددة	المؤشرات	الأولوية	تاريخ بدء التنفيذ
CyAP 1.1	الإيكاو والدول الأعضاء	١-١	٥-٢	إدراج مسألة الأمن الإلكتروني في برامج الإيكاو لمراقبة الأمن والسلامة، بما فيها القواعد القياسية ذات الصلة في برامج التدقيق التي تجريها الإيكاو مثل (برنامج الإيكاو العالمي لتدقيق مراقبة السلامة والبرنامج العالمي لتدقيق أمن الطيران).	إدراج قواعد قياسية ذات صلة بالأمن الإلكتروني في برامج التدقيق التابعة للإيكاو من منظوري الأمن والسلامة.	مرتفعة	مستمر
CyAP 1.2	الإيكاو	١-١	٥-١ انظر أيضاً خطة عمل الأمن الإلكتروني ٤-٦، (الفقرة رقم ٨-٢ من خطة العمل)	إجراء دراسات استقصائية لمبادرات/ممارسات الأمن الإلكتروني لتحديد طريقة إدارة الدول وقطاع الطيران للأمن الإلكتروني في مجال الطيران	نتائج الاستبيانات، عدد المبادرات والأقاليم.	مرتفعة	مستمر
CyAP 1.3	الإيكاو	١-١	٥-١	إعداد حصر بكافة المبادرات المتعلقة بالأمن الإلكتروني المندرجة في عمل جميع مجموعات الخبراء التابعة للإيكاو	تقوم اللجنة الخاصة بتنسيق الأمن الإلكتروني بإعداد وصيانة برنامج عمل الإيكاو للأمن الإلكتروني في مجال الطيران	مرتفعة	٢٠٢٤

CyAP 1.4	الإيكاو والدول الأعضاء	٢-١	٥-٢-٣ و٥-٥ انظر أيضاً خطة عمل الأمن الإلكتروني ٥-١ (الفقرة رقم ٩-٢ من خطة العمل)	أ) وضع نماذج لمذكّرة تفاهم/تعاون واتفاقات خارجية، ب) توفير مبادئ إرشادية بشأن طريقة إعداد هذه الاتفاقات.	توفر نماذج ومبادئ إرشادية	منخفضة	٢٠٢٣ – ٢٠٢٤
CyAP 1.5	الإيكاو والدول الأعضاء وقطاع الطيران	٢-١	٥-٣	وضع مصطلحات متسقة ومتفق عليها تتعلّق بالأمن الإلكتروني في مجال الطيران المدني لتمكين جميع الجهات المعنية في قطاع الطيران، على اختلاف خلفياتها ومستويات أنشطتها، من فهم بعضهام البعض فيما يتعلّق بالأمن الإلكتروني.	نشر مسرد لمصطلحات الأمن الإلكتروني	متوسطة	٢٠٢٣
CyAP 1.6	الإيكاو والدول الأعضاء وقطاع الطيران	٢-١	٥-٤	تتولى الإيكاو وضع إطار مشترك لتحديد الخريطة الوظيفية الرفيعة المستوى التي تصف تبادل المعلومات بين الجهات الفاعلة في مجال الطيران (على سبيل المثال مقدّمو خدمات الملاحة الجوية، شهادة المشغل الجوي، رموز الطائرات، المطارات، الأرصاد الجوية، الصيانة والتصليح والعمرة، الاتصالات والملاحة والاستطلاع) كشرط ضروري لتسهيل فهم ساحة المخاطر الإلكترونية. ستعد الدول الأعضاء وقطاع الطيران مثل هذا الإطار على المستويين الوطني والمؤسسي.	توافر إطار محدد وخريطة عامّة مشتركة لتبادلات المعلومات/التفاعلات في مجال الطيران. خريطة وظيفية لإذكاء الوعي والفهم.	مرتفعة	٢٠٢٤
CyAP 1.7	الإيكاو والدول الأعضاء	٢-١	٥-٧ انظر أيضاً خطة عمل الأمن الإلكتروني ٦-١ (الفقرة رقم ١٠-٢ من خطة العمل)	ستعد الإيكاو نماذج للتعاون فيما بين هيئات الطيران المدني والعسكري من أجل تطويرنماذج/مبادئ توجيهية لكي تستخدم في واجهات الطيران القابلة للتشغيل البيني فيما بين قطاعي الطيران المدني والعسكري، متى أمكن ذلك. تحديد المعايير ومستوى التفاعلات الملائمة.	إتاحة مثل هذه النماذج/المبادئ التوجيهية بشأن التعاون الإلكتروني وقابلية التشغيل البيني فيما بين الطيران المدني والعسكري. قائمة المعايير والحد الأدنى للتفاعلات المطلوبة المنشورة .	مرتفعة	٢٠٢٣
CyAP 1.8	الإيكاو والدول	٣-١	٥-٨	تخطيط وتنظيم ودعم فعاليات دولية وإقليمية للترويج للأمن الإلكتروني في مجال الطيران المدني.	الفعاليات/تعاون دولي لبناء الوعي.	لا ينطبق	مستمر

	الأعضاء وقطاع الطيران						
CyAP 1.9	الإيكاو والدول الأعضاء وقطاع الطيران	١-٣	٥-٤	الحرص على إشراك جميع الجهات المعنية ذات الصلة في المناقشات والأنشطة المتعلّقة بالأمن الإلكتروني في مجال الطيران المدني: المشاركة المستمرة والتواصل مع الجهات المعنية في المجال.	نشر نتائج الجهود المشتركة النشر دليل المشاركات مثل الشراكات والعضوية في الجماعات، إلخ	مرتفعة	مستمر
CyAP 1.10	الإيكاو والدول الأعضاء وقطاع الطيران	١-٢	٥-٢-٢	وضع إطار ثقة خاصّ بالطيران الدولي يمكّن الهيئات من التشغيل البيني فيما بينها بحسب ثقتها بالجهات المعنية الأخرى.	إنشاء إطار ثقة يستخدمه العديد من المنظمات.	مرتفعة	٢٠٢٤-٢٠٢٥

النتائج ذات الأولويّة	**٢- تطوير أساليب الإدارة والمساءلة**
الإجراءات ذات الأولوية	• التشجيع على اعتماد استراتيجيات الإيكاو للأمن الإلكتروني ودعمها والاعتماد عليها. • إعداد المساءلة وأساليب الإدارة على المستوى الوطني للأمن الإلكتروني في مجال الطيران المدني. • ضمان التنسيق على المستوى الوطني فيما بين سلطات الطيران المدني والسلطات الوطنية المختصة في مجال الأمن الإلكتروني. • إنشاء قنوات التنسيق المناسبة فيما بين السلطات الوطنية المتعددة وقطاع الطيران. • تضمين الأمن الإلكتروني في البرامج الوطنية للسلامة ولأمن الطيران المدني. • إدراج الأمن الإلكتروني في الخطط العالمية والإقليمية. • العمل على اعتماد خطة أساسية مشتركة للقواعد والتوصيات الدولية في مجال الأمن الإلكتروني.

الإجراءات

رقم الإجراء في خطّة العمل	**الجهة المعنية**	**الصلة باستراتيجية الأمن الإلكتروني**	**الصلة بالفصل السادس**	**الإجراءات/المهام المحددة**	**المؤشرات**	**الأولوية**	**تاريخ بدء التنفيذ**
CyAP 2.1	الإيكاو والدول الأعضاء		١-٦	وضع هيكل لأساليب الإدارة في ما يتعلّق بالأمن الإلكتروني في مجال الطيران المدني	تحديد الهيكل (الهياكل) الملاءمة لأساليب إدارة الأمن الإلكتروني في مجال الطيران المدني	لا ينطبق	٢٠٢٣

CyAP 2.2	الإيكاو والدول الأعضاء	٢-٢	٦-٣	تتولى الإيكاو إعداد مجموعة عامة من المبادئ حول النظام الملائم (النُظُم الملائمة) لإدارة الأمن الإلكتروني في مجال الطيران المدني. وتتولى الدول الأعضاء تطوير هذه المبادئ على المستوى الوطني متبعة نموذج الإيكاو.	نشر المبادئ العامة	مرتفعة	٢٠٢٣-٢٠٢٤
CyAP 2.3	الإيكاو والدول الأعضاء وقطاع الطيران	٢-٢	٦-٣-٢، أنظر أيضا الفقرة رقم ٨— ١ في خطة العمل	إعداد مواد إرشادية بغية دعم المنظمات في تنفيذ أطر منسَّقة لإدارة الأمن الإلكتروني من أجل دعم تنفيذ نهج نظامي لإدارة مخاطر الأمن الإلكتروني في مجال الطيران، وتقييم فعالية ونضج هذه الأطر.	نشر المبادئ التوجيهية	مرتفعة	٢٠٢٣
CyAP 2.4	الإيكاو الدول الأعضاء	٢-٢	٦-٣	تعزيز آليات التنسيق فيما بين هيئات الطيران المدني والسلطات المسؤولة عن الأمن الإلكتروني	دراسة الإيكاو الاستقصائية – عدد آليات التنسيق الموجودة حالياً.	متوسطة	٢٠٢٢
CyAP 2.5	الإيكاو	٢-٣	٦-٢-١ انظر أيضاً خطة عمل الأمن الإلكتروني ١-٩ (الفقرة رقم ٥-٢ من خطة العمل)	تتولى الإيكاو تضمين الأمن الإلكتروني في الخطط الإقليمية والعالمية من أجل ضمان سلامة منظومة الطيران وأمنها وقدرتها على الصمود في وجه التهديدات والهجمات الإلكترونية	نشر الخطط المحدثة	لا ينطبق	٢٠٢٢ – ٢٠٢٣
CyAP 2.6	الإيكاو		٦-٢	ستُعد الإيكاو سجلا بأفضل الممارسات/مبادئ توجيهية، وسيجري إدراجه في دليل المعلومات.	دليل الإيكاو لأفضل الممارسات	لا ينطبق	٢٠٢٠ – ٢٠٢١
CyAP 2.7	الإيكاو والدول الأعضاء وقطاع الطيران	٣-٢	٦-٣	ستُعد الإيكاو إجراءات نموذجية للإبلاغ عن الوقائع الإلكترونية، بما في ذلك الإرشادات المُتعلِّقة بتصنيف الوقائع. وستُعد الدول الأعضاء وقطاع الطيران إجراءات وطنية وتنظيمية للإبلاغ عن الوقائع الإلكترونية في الوقت المناسب وبطريقة فعَّالة.	إجراءات الإبلاغ عن الوقائع الإلكترونية / عدد الوقائع المبلغ عنها وفقاً للإجراءات.	مرتفع	٢٠٢٢ – ٢٠٢٣
CyAP 2.8	الإيكاو والدول الأعضاء	٢-٢	٦-٢	تقوم الإيكاو بتقييم مدى إدراج الدول الأعضاء للأمن الإلكتروني في برامجها الوطنية لسلامة وأمن الطيران المدني، وخططها للملاحة الجوية	دراسة الإيكاو الاستقصائية – عدد الدول التي أدرجت الأمن الإلكتروني في برامجها الوطنية لسلامة وأمن الطيران المدني	مرتفع	الدراسة الاستقصائية ٢٠٢٢ الإجراءات الأخرى مستمرّ

النتائج ذات الأولويّة	٣- وضع تشريعات ولوائح تنظيمية فعّالة
الإجراءات ذات الأولوية	• ضمان أن تنص المواثيق القانونية الدولية على أطر ملائمة من أجل ردع الوقائع الإلكترونية فضلاً عن محاكمة مرتكبيها. • تحليل التشريعات الوطنية القائمة وتحديث أو اعتماد الملائم منها حسب الضرورة للسماح بردع الهجمات الإلكترونية التي تؤثر في سلامة الطيران المدني أو أمنه أو كفاءته أو استمراريته، والتحقيق فيها وملاحقة مرتكبيها قضائياً. • ضمان توافر التشريعات واللوائح التنظيمية الوطنية الملائمة في ما يتعلَّق بالأمن الإلكتروني في مجال الطيران المدني. • إعداد إرشادات ملائمة تساعد الدول وقطاع الطيران في تنفيذ الأحكام المرتبطة بالأمن الإلكتروني.

الإجراءات

رقم الإجراء في خطّة العمل	الجهة المعنية	الصلة باستراتيجية الأمن الإلكتروني	الصلة بالفصل السابع	الإجراءات/المهام المحددة	المؤشرات	الأولوية	تاريخ بدء التنفيذ
CyAP 3.1	الدول الأعضاء	٣-٣	٧-٤	تصديق الدول الأعضاء على ميثاقي بيجين.	عدد الدول التي صادقت على ميثاقي بيجين	مرتفعة	مستمر
CyAP 3.2	الإيكاو	٣-٣	٧-٣	تحليل مواثيق قانون الجو الدولية	استعراض وتحليل ثغرات مواثيق القانون الجوي الدولي ذات الصلة	مرتفعة	٢٠٢٢
CyAP 3.3	الإيكاو والدول الأعضاء	٣-٣ و٣-٤	٧-٢	تحليل التشريعات الوطنيّة الحالية المُتعلِّقة بالأمن الإلكتروني في مجال الطيران المدني وتحديد الثغرات، بما في ذلك في القانون الجنائي.	دراسة استقصائية عن حالة التشريعات الوطنية في ما يتعلَّق بالتصدّي للأفعال غير المشروعة المرتكبة ضد الطيران المدني عن طريق وسائل إلكترونية.	متوسطة	٢٠٢٣ - ٢٠٢٤
CyAP 3.4	الإيكاو	٣-٣	٧-١	استعراض القواعد والتوصيات الدولية الحالية للإيكاو لتحديد الحاجة إلى إدخال تحديثات ممكنة في مجال الأمن الإلكتروني.	استعراض القواعد والتوصيات الدولية للإيكاو وإجراء تحليل للثغرات فيها	مرتفعة	٢٠٢٢
CyAP 3.5	الإيكاو	٣-٢		استحداث المواد الإرشادية المرتبطة بتنفيذ شروط الأمن الإلكتروني في مجال أمن الطيران واستعراضها وتعديلها	نشر المواد الإرشادية المُتعلِّقة بالأمن الإلكتروني في مجال الطيران المدني	مرتفعة	٢٠٢١ ومستمر

النتائج ذات الأولويّة	٤- وضع سياسة للأمن الإلكتروني						
الإجراءات ذات الأولوية	• ضمان أن يشكل الأمن الإلكتروني جزءا من نُظُم أمن وسلامة الطيران المدني، وكذلك من الأطر الشاملة لإدارة المخاطر. • ضمان إمكانية المقارنة بين المنهجيات المتباينة لتقييم المخاطر المُتعلِّقة بأمن الطيران المدني. • إعداد سياسات الأمن الإلكتروني مع مراعاة دورة الحياة الكاملة لنظم الطيران.						
الإجراءات							
رقم الإجراء في خطّة العمل	**الجهة المعنية**	**الصلة باستراتيجية الأمن الإلكتروني**	**الصلة بالفصل الثامن**	**الإجراءات/المهام المحددة**	**المؤشرات**	**الأولوية**	**تاريخ بدء التنفيذ**
CyAP 4.1	الدول الأعضاء وقطاع الطيران	٤-١	٨-١	ضمان الدول الأعضاء وقطاع الطيران للالتزام من جانب إداراتهم بمعالجة الأمن الإلكتروني في مجال الطيران المدني والقدرة على الصمود في وجه التهديدات والهجمات الإلكترونية.	حملات التوعية/تقديم دليل على الالتزام مثل إقرارات الالتزام، تحديد المسؤوليات في مجال الأمن الإلكتروني في دلائل الإدارة الخاصة بالسلطات والمنظمات	متوسطة	٢٠٢٢ - ٢٠٢٣
CyAP 4.2	الإيكاو والدول الأعضاء وقطاع الطيران	٤-٣	٨-٢، انظر أيضا الفقرة رقم ٥-١١ في خطة العمل	تشجيع البحث والتطوير في مجال الأمن الإلكتروني داخل قطاع الطيران المدني عن طريق التعاون مع الجامعات والمعاهد ودوائر الباحثين، إلخ.	عدد التفاعلات والمشروعات	مرتفعة	٢٠٢٢ - ٢٠٢٣
CyAP 4.3	الدول الأعضاء وقطاع الطيران	٤-٢	٥-٦ و٨-٢	تحديد معايير الأسلوب المشترك فيما بين المؤسسات لتقييم المخاطر، إلى جانب تحديد المعلومات التي ينبغي تبادلها، فضلاً عن المعايير المطلوبة لضمان إمكانية المقارنة بين المخاطر. أما الدول الأعضاء، فستقوم بتحديد تلك المعايير على المستوى الوطني، وسيقوم قطاع الطيران بذلك على المستوى المؤسسي.	نشر أهداف ومعايير التقييم المشترك للمخاطر فيما بين المؤسسات	مرتفعة	٢٠٢٣
CyAP 4.4	الإيكاو والدول الأعضاء وقطاع الطيران	٤-٣	٨-١	وضع سياسة تستند إلى مبدأ "الأمن بفضل التصميم" لتكون أساسا لدورة حياة آمنة لنظم الطيران المدني.	صياغة سياسة لدورة حياة آمنة لنظم الطيران المدني.	متوسطة	٢٠٢٢-٢٠٢٣

CyAP 4.5	الإيكاو والدول الأعضاء وقطاع الطيران	٤-٢	٨-٢	تعقد الإيكاو منتديات دولية من أجل مناقشة الأهداف المتعلقة بالأمن الإلكتروني والقدرة على الصمود في مواجهة التهديدات والهجمات الإلكترونية فيما بين المؤسسات وبين مختلف الوظائف فضلا عن توفير الأحد الأدنى من الوظائف الحيوية في قطاع الطيران المدني. تعقد الدول الأعضاء مثل هذه المنتديات على المستويات الوطنية والإقليمية، ويقوم قطاع الطيران بعقد منتديات خاصة ويشارك على نحو نشط في المنتديات التي تعقدها الإيكاو والدول الأعضاء.	عدد المنتديات المنعقدة لمناقشة الأهداف	مرتفعة	٢٠٢٢-٢٠٢٣
CyAP 4.6	الإيكاو والدول الأعضاء وقطاع الطيران	٤-٣	٨-٢	حصر المبادرات الحالية المعنية بإدارة مخاطر الأمن الإلكتروني في مجال الطيران المدني (بما في ذلك فئات المخاطر، والسيناريوهات، ومعالجة مواطن الضعف، وعمليات تقييم المخاطر).	توافر قاعدة بيانات لمبادرات تقييم المخاطر لأغراض الأمن الإلكتروني	متوسطة	٢٠٢٣-٢٠٢٤
CyAP 4.7	الإيكاو والدول الأعضاء وقطاع الطيران	٤-٣	٨-٣	ستعد الإيكاو قائمة بالسيناريوهات الاستراتيجية للمخاطر الإلكترونية على المستوى الدولي. وستساهم الدول الأعضاء وقطاع الطيران في إعداد وتطوير قوائم مماثلة على المستويين الوطني والمؤسسي.	توافر ١٠ سيناريوهات للمخاطر الإلكترونية	مرتفعة	٢٠٢٣ - ٢٠٢٤
CyAP 4.8	الإيكاو والدول الأعضاء وقطاع الطيران		٨-٢	تحدد الإيكاو فئات المخاطر لكل مجال من المجالات التشغيلية. وستسهم الدول الأعضاء وقطاع الطيران عبر تطوير فئات مماثلة للمخاطر على المستويين الوطني والمؤسسي.	توافر فئات المخاطر	مرتفعة	٢٠٢٣
CyAP 4.9	الإيكاو		٨-٢	إعداد بيان سياق المخاطر العالمية في مجال الأمن الإلكتروني	نشر بيان سياق المخاطر العالمية في مجال الأمن الإلكتروني	مرتفعة	٢٠٢٣

النتائج ذات الأولويّة	**٥- تطوير قدرات تبادل المعلومات**
الإجراءات ذات الأولوية	• إعداد منصات وآليات مُعترفٌ بها لتبادل المعلومات، أو تحسين وتحديث القائم منها، على أن تكون متسقة مع أحكام الإيكاو الحالية بهدف إذكاء الوعي بالأمن الإلكتروني، مما يسمح بمنع حدوث الأحداث المرتبطة بالأمن الإلكتروني والكشف عنها بصورة مبكرة والتخفيف من آثارها. • التأكد من إبلاغ السلطة المختصة بأي واقعة أو نقطة ضعف إلكترونية قد تمثل خطراً كبيراً على سلامة الطيران و/أو أمنه.

الإجراءات							
رقم الإجراء في خطّة العمل	الجهة المعنية	الصلة باستراتيجية الأمن الإلكتروني	الصلة بالفصل التاسع	الإجراءات/المهام المحددة	المؤشرات	الأولوية	تاريخ بدء التنفيذ
CyAP 5.1	الإيكاو	١–٥	١–٩ و٢–٩	تضع الإيكاو إرشادات بشأن تبادل المعلومات.	وثيقة إرشادات لتبادل المعلومات متاحة للمجتمع.	مرتفعة	٢٠٢٢ – ٢٠٢٣
CyAP 5.2	الإيكاو	١–٥	١–٩	تحدد الإيكاو، بدعم من دولها الأعضاء وقطاع الطيران، تبادل المعلومات المرتبطة بالأمن الإلكتروني والاحتياجات من حيث التعاون (بما في ذلك على سبيل المثال لا الحصر في أوقات الأزمات) والسياسات اللازمة في هذا الصدد.	وضع قائمة بالمعلومات التي يُحتمل تبادلها	متوسطة	٢٠٢٢ – ٢٠٢٤
CyAP 5.3	الإيكاو	١–٥	١–٩	إعداد إرشادات بشأن استخدام بروتوكول إشارات المرور (TLP) لتحديد مستوى التوزيع/التقييد لدى توزيع ومواصلة تبادل المعلومات الإلكترونية.	نشر الإرشادات بشأن سياسة استخدام بروتوكول إشارات المرور (TLP) لدى توزيع المعلومات الإلكترونية وتبادلها.	مرتفعة	٢٠٢١
CyAP 5.4	الإيكاو والدول الأعضاء وقطاع الطيران	٢–٥	٢–٩	النظر في جدوى تحديد معايير الإفصاح المسؤول عن مواطن الضعف المُتعلِّقة بالأمن الإلكتروني.	توفّر ونشر مبادئ الإفصاح المسؤول عن مواطن الضعف إذا اعتُبر ذلك مجدياً.	مرتفعة	٢٠٢٣
CyAP 5.5	الإيكاو والدول الأعضاء	٢–٥	٤–٩	تقوم الإيكاو بإنشاء وتحديث شبكة لجهات الاتصال على المستوى الدولي تُعنى بالمسائل المتعلّقة بالأمن الإلكتروني في مجال الطيران المدني لدى الدول الأعضاء وقطاع الطيران. تتعاون الدول الأعضاء مع الإيكاو عن طريق إنشاء مثل هذه الشبكة لجهات الاتصال على المستوى الوطني.	إقامة شبكة لجهات الاتصال المعنية بالأمن الإلكتروني في مجال الطيران المدني. نشر شبكة جهات الاتصال الخاصة بكل دولة عضو.	متوسطة	٢٠٢٤ – ٢٠٢٥

النتائج ذات الأولويّة	٦- تطوير إدارة الوقائع والتخطيط للطوارئ						
الإجراءات ذات الأولوية	• ضمان توافر الخطط المناسبة والقابلة للتوسع لتوفير استمرارية سلامة عمليات الطيران المدني وأمنها في حالة حدوث وقائع إلكترونية. • ضمان تحديث خطط الطوارئ الحالية من أجل إدراج أحكام خاصة بالتصدِّي للوقائع المُتعلِّقة بالأمن الإلكتروني والتعافي من آثارها، وتنفيذ تمارين منتظمة/دورية لاختبار القدرات على كشف الوقائع الإلكترونية والتصدِّي لها والتعافي من آثارها.						
الإجراءات							
رقم الإجراء في خطّة العمل	**الجهة المعنية**	**الصلة باستراتيجية الأمن الإلكتروني**	**الصلة بالفصل العاشر**	**الإجراءات/المهام المحددة**	**المؤشرات**	**الأولوية**	**تاريخ بدء التنفيذ**
CyAP 6.1	الدول الأعضاء وقطاع الطيران	١-٦	١-١٠	تحدد الدول الأعضاء الأهداف والمستويات الدنيا من الوظائف الهامة لقطاع الطيران المدني. يتولى قطاع الطيران تنفيذ الأهداف التي تم وضعها.	نشر قائمة بالأهداف والمستويات الدنيا المقبولة من الوظائف لاستمرارية الطيران	مرتفعة	٢٠٢٢ – ٢٠٢٣
CyAP 6.2	الإيكاو والدول الأعضاء	١-٦	٢-١٠	تعد الإيكاو الإرشادات والعمليات بغية إدراج الجهات المعنية العسكرية في مجال التخطيط للتصدي لوقائع الأمن الإلكتروني في مجال الطيران المدني. وتقوم الدول الأعضاء بإعداد إجراءات واتفاقات تعاون فيما بين سلطات الطيران المدني والعسكري.	إعداد ونشر إرشادات بشأن عمليات وإجراءات التعاون المدني–العسكري في ما يتعلَّق بالتصدِّي لوقائع الأمن الإلكتروني في مجال الطيران المدني	مرتفعة	٢٠٢٢ – ٢٠٢٣
CyAP 6.3	الإيكاو والدول الأعضاء وقطاع الطيران	١-٦	١-١٠	تعد الإيكاو إرشادات بخصوص قدرات التصدي لوقائع الأمن الإلكتروني في مجال الطيران المدني والتعافي منها، بما في ذلك خطط الطوارئ والاستجابة للحالات الطارئة. وتتولى الدول الأعضاء وقطاع الطيران، استنادا إلى إرشادات الإيكاو، تطوير مثل هذه الإرشادات على المستويين الوطني والمؤسسي.	نشر الإرشادات المتعلقة بقدرات التصدي لوقائع الأمن الإلكتروني في مجال الطيران والتعافي منها، بما في ذلك خطط الطوارئ والاستجابة للحالات الطارئة.	مرتفعة	٢٠٢٢ – ٢٠٢٣
CyAP 6.4	الدول الأعضاء	١-٦	٢-١٠ و٣-١٠	تعد الدول الأعضاء وتنفذ القدرات والخطط المرتبطة بالكشف عن وقائع الأمن الإلكتروني في مجال الطيران وتحليلها والتصدي لها على المستوى التشغيلي.	استقصاء لمتابعة مستوى التنفيذ	مرتفعة	٢٠٢٣ – ٢٠٢٤

CyAP 6.5	الإيكاو والدول الأعضاء	٦-١	١٠-١	وضع عمليات للتنسيق لدى وقوع أزمات أمن إلكتروني في مجال الطيران المدني، بما في ذلك التنسيق على المستوى الوطني والدولي.	وضع تعريف لعمليات تنسيق أزمات الأمن الإلكتروني. نشر مواد إرشادية	متوسطة	٢٠٢٤ – ٢٠٢٥
CyAP 6.6	الدول الأعضاء وقطاع الطيران	٦-١	١٠-٣	المواظبة على إجراء جلسات محاكاة مكتبية دورية وتمارين حية.	تبادل الدروس المستفادة حسب الاقتضاء.	مرتفعة	٢٠٢٢-٢٠٢٣

النتائج ذات الأولويّة	**٧- تطوير بناء القدرات والتدريب وثقافة الأمن الإلكتروني**
الإجراءات ذات الأولوية	• ضمان توافر المهارات لدى العاملين، على أساس دور كلٍ منهم، في مجال الطيران والأمن الإلكتروني. • تعزيز مستوى الوعي بالأمن الإلكتروني، بما في ذلك الأنشطة المُتعلِّقة بالتأسيس للنظافة الإلكترونية الملائمة. • ضمان إدراج مناهج الأمن الإلكتروني في الطيران ضمن الأطر التعليمية الوطنية على مستوى التطوير المهني، وذلك من أجل ضمان توافر مجموعة شاملة من المعارف حول أمن الطيران وسلامته على نطاق المنظمة، بما في ذلك كوادر الإدارة العليا بها. • تعزيز الابتكار في مجال الأمن الإلكتروني والترويج لإطلاق البحث والتطوير المناسبين. • تضمين الأمن الإلكتروني في استراتيجية الإيكاو للجيل القادم من المهنيين العاملين في مجال الطيران.

الإجراءات

رقم الإجراء في خطّة العمل	**الجهة المعنية**	**الصلة باستراتيجية الأمن الإلكتروني**	**الصلة بالفصل الحادي عشر**	**الإجراءات/المهام المحددة**	**المؤشرات**	**الأولوية**	**تاريخ بدء التنفيذ**
CyAP 7.1	الإيكاو والدول الأعضاء وقطاع الطيران	٧-١	١١-١	تعريف ثقافة الأمن الإلكتروني في مجال الطيران المدني والتوعية بشأنها والترويج لها.	توافر الدورات التدريبية والمواد الإرشادية المرتبطة بثقافة الأمن الإلكتروني في مجال الطيران المدني.	متوسطة	٢٠٢٢ – ٢٠٢٣
CyAP 7.2	الدول الأعضاء وقطاع الطيران	٧-٢	١١-١	تقوم الدول الأعضاء وقطاع الطيران بتحديد الشروط المناسبة على أساس الدور، للتدريب على الأمن الإلكتروني في مجال الطيران على كافة المستويات ضمن منظماتها.	إعداد التدريب المناسب على أساس الدور في مجال الطيران والأمن الإلكتروني	مرتفعة	٢٠٢٢ – ٢٠٢٣
CyAP 7.3	الإيكاو والدول الأعضاء	٧-٣	١١-١	تدرج الإيكاو الأمن الإلكتروني في استراتيجيتها للجيل القادم من المهنيين العاملين في مجال الطيران. وتدرج الدول الأعضاء الأمن الإلكتروني في استراتيجياتها الوطنية	إدراج الأمن الإلكتروني في استراتيجيات الجيل القادم من المهنيين	متوسطة	٢٠٢٢ – ٢٠٢٣

			المرتبطة باستراتيجية الجيل القادم من المهنيين العاملين في مجال الطيران.			العالمين في مجال الطيران	
CyAP 7.4	الإيكاو	٣-٧	١-١١	تُجري الإيكاو تحليلاً لوسائل وطرق دعم مُتطلَّبات الكفاءة على أساس الدور في ما يتعلق بالأمن الإلكتروني	إدراج التدريب على الأمن الإلكتروني على أساس الدور في وثيقتي الإيكاو رقم Doc 7192 وDoc 9868 إذا اعتُبر ذلك مجدياً.	مرتفعة	٢٠٢٣ - ٢٠٢٥
CyAP 7.5	الإيكاو والدول الأعضاء وقطاع الطيران	٣-٧	١-١١	تطوير أنشطة بناء القدرات	إتاحة دورات تدريبية على الأمن الإلكتروني في مجال الطيران.	مرتفعة	مستمر

— انتهى —