AN-Conf/13-WP/270
28/9/18
English, Arabic, Chinese[1], French, Russian and Spanish only[2]

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

مفهوم منظومة النظم للأمن السيبراني في الطيران

(ورقة مُقدَّمة من كندا والنمسا عن الاتحاد الأوروبي ودوله الأعضاء[3]، والدول الأعضاء الأخرى في اللجنة الأوروبية للطيران المدني[4] والمنظمة الأوروبية لسلامة الملاحة الجوية وسنغافورة وشاركت في تقديمها أستراليا ونيوزيلندا)

الموجز التنفيذي

تطرح هذه الورقة باختصار مفهوم منظومة النظم وتطرحه كحل مناسب لاعتبارات الأمن السيبراني في الطيران المدني كما ستقدم هذه الورقة مفهوم الأمن في التصميم وكيف سيسهم ادماج هذا المفهوم في منظومة الطيران المدني في جعله أكثر تحصينا وقدرة على التعافي.

الإجراء:

المؤتمر مدعو للموافقة على التوصية التي تشملها الفقرة الثالثة.

١- المقدمة

١-١ يعتبر توفر المعلومات الدقيقة والأداء الصحيح لأنظمة السلامة الحرجة من متطلبات سلامة وأمن الطيران المدني، القطاع الذي يخضع للمزيد من التقنيات الرقمية. ان منظومة الطيران المدني متكاملة بشكل كبير وتتدفق معلوماته على نطاق عالمي ولذلك مبادرات الأمن السيبراني يجب أن تكون شمولية من جميع النواحي.

١-٢ ان الشمولية يمكن لها النجاح فقط في ظل منظومة النظم والتي يقوم من خلالها جميع أعضاء مجتمع الطيران بالتشارك في المسؤولية، ان نظام الطيران المشتمل على العديد من الشبكات والمعدات آخذ في التواصل بحيث تعتمد مكوناته

[1] الإصدار باللغة الصينية مقدم من سنغافورة.

[2] الإصدارات الإنجليزية والعربية والفرنسية والروسية والإسبانية مقدمة من كندا.

[3] النمسا وبلجيكا وبلغاريا وكرواتيا وقبرص والجمهورية التشيكية والدانمرك وإستونيا وفنلندا وفرنسا وألمانيا واليونان وهنغاريا وآيرلندا وإيطاليا ولاتفيا وليتوانيا ولكسمبرغ ومالطة وهولندا وبولندا والبرتغال ورومانيا وسلوفاكيا وسلوفينيا وإسبانيا والسويد والمملكة المتحدة.

[4] ألبانيا وأرمينيا وأذربيجان والبوسنة والهرسك وجورجيا وآيسلندا وجمهورية مولدوفا وموناكو والجبل الأسود والنرويج وسان مارينو وصربيا وسويسرا وجمهورية مقدونيا اليوغسلافية السابقة وتركيا وأوكرانيا.

على بعضها البعض في تبادل المعلومات والبيانات الرقمية في ذات الوقت الذي يعتمد فيه الشركاء كالدول والطائرات والمطارات ومزودي خدمات الملاحة الجوية على تقنية معلومات واتصالات مشتبكة للقيام بمهامهم اليومية.

١-٣ ان التطورات المتمثلة في نظام إدارة المعلومات الشامل والطائرات دون طيار وبروز مستخدمين مستقبليين للمجال الجوي وغيرهم من الشركاء المحتملين يزيد من اعتمادية مكونات المنظمة بعضها على بعض، ومن هذا المنطلق تبرز حاجة نظام الطيران المستقبلي الى تناغم اكثر في التصميم وقدراً اقل من اعمال التطوير الفردية للحفاظ على تحصينه ضد التهديد السيبراني.

١-٤ بالإضافة للتحديات السابقة الذكر فان التطورات الحاصلة في أنظمة المعلومات وترابطها قد أدى الى بروز فجوات أخرى، ان احداث التهديد السيبراني من شأنها التأثير على الطيران على مستويات متعددة وعلى أداء منظومة الملاحة الجوية وسلامة الطيران ككل، ان احداثا كهذه تؤثر على تبادل المعلومات بين الشركاء مما يؤثر بشكل مباشر على السلامة، الأمن، القدرة الاستيعابية والفعالية وما قد يتبعها من عواقب جسيمة محتملة.

٢- المناقشة

٢-١ **الطيران كمنظومة نظم – (SoS)** في قطاع الطيران، يلعب العديد من الشركاء، سواء المباشرين أو غير المباشرين، دوراً في تشغيل واستدامة النظم الفرعية الفردية والنظام ككل – مع إدراك أمكانية أن يتكون النظام من منتجات وأشخاص وعمليات. كل من هذه الأنظمة الفرعية تنبثق مباشرة من أنظمة فرعية أخرى لكي تعمل بسلاسة وكفاءة ؛ وبالعكس، فإن لكل نظام من هذه الأنظمة الفرعية أيضاً تأثيراً كبيراً على الأنظمة الفرعية الأخرى عندما يتعذر عليها العمل بشكل صحيح.

٢-٢ هذه الأنظمة الفرعية اليوم مصممة ومتكاملة ومشغلة ومدارة بشكل مستقل عن بعضها البعض، وتتطور بنمط فردي، مما يؤدي إلى عملية تطور شاملة تمثل تحدياً للتنبؤ بها وتحديدها بشكل حاسم. بما أن الشركاء في مجال الطيران يتحملون مسؤولية كاملة عن النظام ككل، فإن اعتبار الطيران كمنظومة أنظمة هو أكثر أهمية. ومن ثم، فإن المسؤولية عن أداء نظام الطيران تشمل كل من الشركاء المباشرين مثل الطائرات ومالكي/مشغلي المطارات ومقدمي خدمات الملاحة الجوية، وكذلك الشركاء غير المباشرين مثل الدول ومصنعي/مصممي المعدات.

٢-٣ نظراً لأن هذه الأنظمة الفرعية تخدم وظائف فردية متسلسلة لتحقيق أهداف مشتركة (مثل الاتصالات بين التحكم في الحركة الجوية والطيار، أو بيانات تتبع الموقع بين مراكز التحكم في تشغيل الطائرات والطائرات)، فإن تضارب أي من هذه الأنظمة الفرعية قد يؤدي إلى حدوث ضرر يؤثر على الوظيفة العامة لسلسلة النظم الفرعية ككل. وعلى هذا النحو، يجب معالجة إدارة مخاطر الأمن السيبراني باستخدام نهج شامل من أجل الحد من إمكانية وصول عوامل التهديد إلى الوظائف الأساسية.

٢-٤ **الأمن السيبراني: اعتبارات مستمرة آخذة في التطور** – بالنظر إلى الطبيعة التطورية لمنظومة الأنظمة الموصوفة أعلاه، يجب أن يكون الأمن السيبراني أيضاً أمراً بنفس الأهمية لدى الشركاء المختلفين في نظم الأنظمة في الطيران. ومن الضروري أيضاً أن تحافظ أنظمة الملاحة الجوية على شروط الأمن السيبراني المطلوبة من خلال توفير قدر كاف من المرونة والقدرة على التكيف عندما تتفاعل مكوناتها بشكل دائم مع بطرق متعددة مع بعضها البعض (على سبيل المثال، الطائرات تتفاعل مع مختلف مقدمي خدمات الملاحة الجوية أثناء مرورها عبر مختلف مناطق معلومات الطيران).

٢-٥ لذلك، يتطلب تطوير وصيانة مثل هذه المناعة الإلكترونية عبر منظومة الأنظمة التنسيق المستمر بين جميع الشركاء (انظر الفقرة ٢-٢)، من أجل الحفاظ على المرونة والقدرة على التكيف اللازمة لنمو منظومة أنظمة تعمل بشكل صحيح.

٢-٦ من التحديات المهمة التي يجب مواجهتها لتحقيق هذا الهدف هو مفهوم "التركيب – القدرة على دمج عناصر متعددة (مكونات للأنظمة، أو أنظمة فرعية لأنظمة الأنظمة) في كيانات أكبر بشكل آمن. ويتمثل التحدي الرئيسي هنا في الخروج عن نموذج السلامة، حيث يتركز دمج العناصر في المقام الأول على وظائفها وعلاقاتها عبر الواجهات المشتركة. من منظور الأمن السيبراني، يتطلب تكامل العناصر الفردية أيضاً دراسة متأنية لكيفية إسهام الأوضاع الأمنية لكل عنصر في الحالة العامة للأمن السيبراني. إن أحد الأسئلة الرئيسية التي ستظهر في هذا السعي تتضمن كيفية دعم الدول والمناطق (وغيرها من الشركاء) في سعيهم للتنمية بحيث يمكن حماية منظومة الأنظمة بشكل فعال من هجمات الأمن السيبراني، على الرغم من التباين الحتمي الذي سيحدث بين الأنظمة الفرعية.

٢-٧ بتحقيق الهدف المذكور أعلاه، سيتطلب دمج الأنظمة الفرعية الفردية دراسة متأنية لربط بيئات الأمن المحلية لكل نظام فرعي، إلى الحد الذي تظهر فيه بيئة مرنة وشاملة. يمكن أن تؤدي المنهجيات غير المنسقة للأمن السيبراني إلى تكوين نقاط ضعف غير مكتشفة في الحماية ؛و تداخلات في دفاعات الأنظمة وهو الأمر الذي له نفس القدر من الخطورة، لأن هذا السيناريو من المحتمل أن يؤدي إلى خلق ثغرات لهجوم محتمل على منظومة الأنظمة في الطيران.

٢-٨ لذلك، فإن اتباع نهج منسق عالمياً لإدارة تفاعل النظام أمر ضروري، ويمثل جوهر ذلك الهدف رؤية مشتركة لكيفية تفاعل هذه الأنظمة والأنظمة الفرعية.

٢-٩ **دمج الامن في تصميم أنظمة الطيران** – من أجل ان تحقق منظومة الأنظمة في الطيران المستوى المطلوب من المقاومة السيبرانية، فمن المهم لاعتبارات الأمن السيبراني إدراجها من بداية تطوير النظام، بدلا من التي يجري النظر فيها بأثر رجعي. وهذا من شأنه أيضاً أن يسمح بمراعاة الاعتبارات بين النظم الفرعية، بحيث تتم هذه التعاملات بطريقة آمنة وفعالة.

٢-١٠ تركز معظم معايير الأمن الحالية على التدابير الاحترازية المتخذة والمطبقة ضمن السياق التنظيمي – هناك حاجة ملحة إلى تعديل تركيز هذه التدابير لتشمل التدابير التي ينبغي أخذها من المنظور المشترك بين المنظمات وحصرها كذلك. يسمح ذلك بضمان أمن منظومة الأنظمة العام بشكل عام، علاوة على الأمان الناشئ عن دمج الأنظمة الفرعية المؤمنة بشكل فردي.

٢-١١ بدون إدارة مناسبة، يمكن أن تشكل النهج غير المنسقة في مجال الأمن السيبراني في الأنظمة الفرعية للطيران خطراً على النظام ككل. كما ينبع عدم التنسيق هذا من عدم توافر اتصال كافي بين مديري النظم الفرعية وغيرهم من الشركاء المعنيين أثناء تطوير وتصميم مناهج الأمن السيبراني.

٢-١٢ سوف تساهم الدول في منظومة نظم الطيران الذي يحافظ على الدفاع المتعمق من خلال مستويات تنسيق متعددة (مثلاً بين الدول كمدراء لنظم الطيران المحلية، ومدراء الأنظمة الفرعية داخل أنظمة الطيران المحلية، وما إلى ذلك) عبر مستويات مختلفة من الأنظمة الفرعية، وأيضاً عبر ضمان الحماية الفعالة للأنظمة الفرعية المستقلة في حد ذاتها.

٢-١٣ **العمل المستقبلي** – لا ينبغي أن يحل العمل في دمج الأمن بالتصميم كجزء من التصميم المبدئي لنظام ما محل أفضل الممارسات التي اكتسبها مجتمع الطيران من خلال عقود طويلة من الخبرة في تطوير أنظمة الطيران والعمل على تحديات الأمن السيبراني. من خلال دمج هذه المبادئ جنباً إلى جنب مع التركيز التقليدي على مدى تحمل النظام للخلل، بالإضافة إلى التركيز على زيادة سهولة الوصول إلى البيانات والنظم التشغيلية، سيعزز الشركاء منظومة نظم الطيران من خلال سياساتها المتعلقة بالمرونة الإلكترونية، مع الحفاظ على الفعالية التشغيلية.

٢-١٤ كجزء من تنوع المفاهيم والحلول التشغيلية التي تجري مناقشتها في مختلف محافل الطيران اليوم، من المهم أن تأخذ الدول والمصنعين في الاعتبار الاعتبارات المذكورة أعلاه من خلال عملية التطوير والتصميم. وبالتالي، قد يقوم المجتمع أيضاً

بتطوير عمله الجماعي من أجل تحديد الأنظمة الفرعية والأبحاث التي تمثله، حيث تمتد نتائجها – بناءً على إلى التدابير المتخذة والممارسات المستخدمة – إلى أنظمة فرعية أخرى لتحسين المرونة السيبرانية عبر النظام.

٢-١٥ وبالمثل، بعد النجاح في هذا المجال، قد ينظر مجتمع الطيران في العمل على البدء في تطوير المزيد من الأنظمة الفرعية المتزايدة، والتي تأخذ أمن المعلومات في الاعتبار أثناء مرحلة التصميم الأولية. ومع تقدم هذا العمل ونضوجه، قد يبدأ الشركاء بشكل جماعي باكتشاف ما إذا كان هناك مرشحين مناسبين وموثوقين يتم تكليفهم بمسؤولية تطوير وصيانة مثل هذه الأنظمة الآمنة عن طريق التصميم، وإمكانية تنفيذ مثل هذه العمليات في نظام الطيران المستقبلي.

٢-١٦ من خلال الاستمرار في الاستثمار وتكريس الجهود في مجال مناعة النظام السيبراني، سوف يسهم مجتمع الطيران بفعالية في التشغيل الآمن والكفؤ للنظام البيئي للطيران (منظومة النظم) في المستقبل.

٣- الاستنتاجات

٣-١ يُرجى من المؤتمر أن يوافق على التوصيات التالية:

أ) حث الإيكاو والدول على تقدير أهمية كون المناعة السيبرانية لنظام الطيران تعتمد على التنسيق المستمر بين جميع الشركاء المعنيين؛

ب) مطالبة منظمة الطيران المدني الدولي بالاعتراف بمفهوم "منظومة الأنظمة"، الذي يتطلب ضرورة التعاون والتنسيق بين مديري النظم الفرعية، خاصة عند تطوير الأنظمة الفرعية "الآمنة حسب التصميم" ودمجها وتشغيلها وصيانتها؛

ج) حث الإيكاو على وضع إطار يتطلب من الدول ويوجهها لتنفيذ تدابير لتقليل التهديد السيبراني والمخاطر على أنظمة الطيران المدني. وقد يؤدي ذلك إلى تحديد SARPs لعدد من الملاحق المتأثرة بالإيكاو؛

د) الاعتراف بالمفاهيم الواردة في ورقة المعلومات: الاعتبارات المتعلقة بالأمن السيبراني في مجال الطيران.

–انتهى–