الحماية القانونية للطيران المدني ضد الجرائم السيبيرانية

The Legal protection of civil aviation from cybercrime

مناد اشراق[1]، هارون أوروان[2]

[1] طالبة دكتوراه بكلية الحقوق والعلوم السياسية، جامعة يحي فارس –المدية-،

[1] مخبر السيادة والعولمة، menad.icherak@univ-medea.dz

[2] أستاذ محاضر -أ- بكلية الحقوق والعلوم السياسية، جامعة يحي فارس –المدية-،

[2] مخبر السيادة والعولمة، ourouane.haroun@univ-medea.dz

تاريخ الإرسال: 2020/02/21 تاريخ القبول:08/ 2020/05 تاريخ النشر: 28/ 2021/05

ملخص:

هدفت هذه الدراسة إلى تسليط الضوء على الجرائم السيبيرانية المستهدفة لأمن وسلامة الطيران المدني والإحاطة بكافة جوانبه النظرية والقانونية، يعد هذا النوع من الجرائم من أخطر الجرائم الحديثة التي تكبد مؤسسات الطيران المدني خسارات كبيرة مادية وبشرية، فهذا النوع من الجرائم يمس أساسا بنظم المعلومات التي يعتمد عليها الطيران كثيرا على نطاق واسع كما توصلت الدراسة الدراسة إلى جملة من النتائج أهمها: أن الجرائم السيبيرانية جرائم ماسة بالأمن السيبيراني، كما أنها جرائم متنوعة ومتعددة بذل المجتمع الدولي جهودا من أجل السيطرة عليها وتأطيرها قانونيا، كما أوصت الدراسة بضرورة إيجاد القوانين والساسات اللازمة للحد من هذه الجرائم لما لها من الآثار السلبية تقلل من مصداقية وسمعة الطيران المدني .

الكلمات المفتاحية: الجرائم السيبيرانية، الطيران المدني، الامن السيبراني،الجهود القانونية.

Abstract:

This study aimed to put the light on cybercrime targeting the security and safety of civil aviation and take note of all its theoretical

and legal aspects. this type of crime is one of the most dangerous modern crimes that incur civil aviation institutions large material and human losses, this type of crime mainly affects the information systems that depend on it flying a lot on a large scale, and the study also reached a set of results, the most important of which are: that cybercrime are crimes against cyber security, as they are various and multiple crimes that the international community made efforts to control and legalize, as recommended the study of the need to find the necessary laws to curb these crimes because of its negative effects reduce the credibility and reputation of civil aviation.

***Key words**: cybercrime, civil aviation, cyber security, legal efforts.*

1- المؤلف المرسل: مناد إشراق، **الإيميل:** menad.icherak@univ-medea.dz

مقدمة :

يعد قطاع النقل العام بكافة فروعه من أهم القطاعات الاقتصادية الحساسة في الدول نظرا لارتباطه الوثيق بالاقتصاد والتنمية، حيث تتعدد وتتنوع فروع هذا القطاع بتنوع وسائل النقل المستعملة فيه، ومن أهم هذه الفروع نجد قطاع الطيران المدني، الذي شهد ولازال يشهد قفزة نوعية وتطورا كبير منذ بداية القرن المنصرم وإلى غاية يومنا هذا، وهذا كله بسبب تطورصناعات وسائل النقل الجوي المتزامن بظهور شركات النقل التجاري الجوي.

يعد قطاع الطيران المدني من القطاعات الحساسة جدا في النقل وهذا بسبب دخوله في كافة المجالات الحياتية، كمجال السفروالمجال التجاري، وهذا القطاع وكغيره من القطاعات التجارية، يتعرض إلى العديد من التهديدات التي تمس بأمنه وسلامته.

ونظرا للأهمية التي تعتري هذا الأخير إزداد إهتمام أشخاص المجتمع الدولي بهذا القطاع وهذا من أجل حمايته من كل الأخطار التي قد تصيبه فقاموا بإنشاء هيئات دولية وإقليمة وحتى وطنية مختصة بهذا القطاع، كما قاموا أيضا بعقد المؤتمرات والمصادقة على الإتفاقيات والقوانين الخاصة بالطيران المدني.

ومع التطور الهائل الذي حدث في تكنلوجيا المعلومات والإتصال كتكنلوجيا الأنترنت، ودخولها في مجال الطيران المدني بصورة كبيرة جدا، ظهر نوع جديد من التهديدات الماسة بأمن وسلامة الطيران المدني، والمسمى بالجرائم السيبيرانية، هاته الجرائم المستهدفة لهذا القطاع والمكبدة لخسائر كبيرة جدا فيه.

نظرا لحداثة هذه الجرائم نجد نقصا كبيرا في الجانب الجزائي الخاص بها، هذا الجانب الذي يضبط ويقر الحماية لهذا القطاع ضد هذا النوع من الجرائم. وهذا مايجعلنا نطرح الإشكال التالي: ما مدى تأثير الجرائم السيبيرانية على أمن وسلامة الطيران المدني؟

من أجل الإجابة على هذا الإشكال اعتمدنا خطة مقسمة إلى محورين:

المحور الأول بعنوان: التأصيل النظري للجرائم السيبيرانية المهددة للطيران المدني، اما المحور الثاني فبعنوان: الجهود الدولية في مكافحة الجرائم السيبيرانية المهددة لامن وسلامة الطيران المدني.

معتمدين في ذلك على المنهج الوصفي التحليلي لكونه المنهج المناسب لهذا النوع من الدراسة.وهذا من أجل بلوغ الهدف المرجو من هذه الدراسة ألاوهو تسليط الضوء على الجرائم السيبيرانية الماسة بأمن وسلامة الطيران وإستعراض بعض الهيئات التي تعنى بمحاربة هذا النوع من الجرائم والحفاظ على أمن وسلامة الطيران المدني.

1. المحور الاول:التأصيل النظري للجرائم السيبيرانية المهددة للطيران المدني

يتعرض قطاع الطيران المدني كغيره من باقي القطاعات الحساسة الى العديد من التهديدات التي تمس بأمنه وسلامته وتتعدد وتتنوع هذه الجرائم كما تتميز بالتطور السريع ومن اهم الجرائم الحديثة المهددة لهذا الاخير هي الجرائم السيبيرانية.

فهاته الاخيرة تشكل خطورة كبيرة على الطيران المدني وذلك بسبب تعدد اشكالها وانواع المهاجمين فيها ودوافعهم.

ولهذا ارتأينا تقسيم هذه المحورعلى النحو التالي:

1.1. الأمن السيبيراني في مجال الطيران المدني

هناك علاقة وطيدة بين قطاع الطيران المدني و الامن السيبراني وهذا بسبب دخول التكنولوجيا وبشكل كبير في هذا القطاع ولهذا سنقوم بدراسة مايلي:

1.1.1.الأمن السيبيراني:

يمكن تعريف الأمن السيبيراني على أنه مجموعة من الأدوات والسياسات والضمانات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والتدريب وأفضل

الممارسات والضمان والتقنيات المستخدمة لحماية البيئة السيبيرانية وأصول المنظمات[1]

ويعني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى للمحافظة على سرية المعلومات الالكترونية، ومنع الاختراقات الفيروسية من اجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة ، وفي الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على[2]

حد سواء، خصوصاً بعد الثورة الهائلة في عالم الاتصالات والتداولاتالالكترونية شكل هكذا نوع من الأمن هاجس[3]إستراتيجي للقوى العالمية والمتمثلة بالولايات المتحدة والصين وروسيا فتدور اليوم حرب الكترونية بين هذه القوي من اجل الاختراق المعلومات والتأثير على اسعار البورصة والعملات.

حيث تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيات الاتصالات والمعلومات المتصلة بالشبكة العالمية غير أن هذا الاعتماد المطرد ترافقة مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع المعلوماتي وأعضائه.

إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية[4].

2.1.1 الأمن السيبيراني والطيران المدني:

"يعتمد الطيران على النظم الحاسوبية على نطاق واسع في العمليات البرية والجوية وادارة الحركة الجوية..... "

وكما هو الأمر في العديد من الانشطه البشرية المعقدة الأخرى، فان [5] استخدام تكنولوجيا المعلومات والإتصال في الطيران المدني تزايد أضعافا مضاعفة على مدى السنوات الأخيرة، من التنمية والبناء، من الطائرات إلى أدوات الاتصالات والملاحة، جنبا إلى جنب مع جميع آلاف الاتصالات التي تربط أجزاءا مختلفه من المطار. كما هو الحال في غيرها من الحقول، والرقمنة

والتنسيب على الإنترنت من هذه الأجهزة المعقدة أدخلت مشاكل كبيره مرتبطة بالأمن السيبيراني[6] .

3.1.1.تعريف الجرائم السيبيرانية:

تعرف الجرائم السيبيرانية بأنها: «أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب. »[7]

كما تعرف بانها:« الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً. »

وكما جاء في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام 2000 م تعريف الجرائم المعلوماتية حيث ورد فيه أنه:

«يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية.[8] تلك الأفعال التي تمثل الإعتداء على مصلحة محمية بموجب الشرع أو النظام أو القانون، عن طريق التعدي على النظام المعلوماتي، أوإستخدامه في ارتكاب الجرائم، أوإيصالها إلى المتلقي، بهدف تحقيق مصلحة معينة أو الإضرار بالغير، ويقوم بهذه الأفعال أشخاص لهم دراية باستخدام النظام المعلوماتي». [9]

2.1. تقسيمات الهجمات السيبيرانية والمهاجمين السيبيرانين:

نظرا لتعدد الهجمات السيبيرانية المهددة لسلامة الطيران المدني وتنوعها بالموازاة مع تنوع مرتكبي هذا النوع من الجرائم ارتئينا تقسيم هذه النقطة إلى:

2.2.1.أنواع التهديدات السيبيرانية الرئيسة الماسة بامن وسلامة الطيران المدني:

تتعد أنواع وأشكال التهديدات السيبيرانية الماسة أساسا بأمن وسلامة الطيران المدني والتي سنتناولها كما يلي :

- **هجمات التصيد الإحتيالي:**

هجمات التصيد الإحتيالي هي في المقام الأول خطوة مسبقة إلى هجوم خبيث موجه بشكل كامل نحو مؤسسة. والهدف الرئيسي هو الحصول على بيانات اعتماد المستخدم من خلال تقنيات الهندسة الاجتماعية والتسلل إلى نظام الوكالة لزرع وإطلاق التهديدات المتقدمة المستمرة.وقد وقع عدد من المنظمات، بما في ذلك المطارات، ضحية لهذه الهجمات.[10]

- **الهجمات المستندة إلى WiFi:**

ما لم يتم تأمينها بشكل كاف، فإن أنظمة الواي فاي التقليدية المتوفرة علي متن الطائرات تكون ضعيفه ويمكن للجهات الفاعلة الخبيثة استخدامها لاختراق معدات إلكترونيات الطيران على متنها وتعطيل أو تعديل الاتصالات الساتلية. وهناك اطار رمز حقن من قبل الجهات الفاعلة الخبيثة.

يمكنأن تحصل على الأرجح في نظام الطائرة وتجاوز تطبيقات أمنية تؤدي إلى إمكانيات كارثية مثل الإختطاف و/أو التحطم في الجو.. الخ.

- **BYOD :**

تسمح أنظمه الترفيه الحالية في الطيران للركاب بمشاهدة مقاطع الفيديو الخاصة بهم عن طريق USB.

وما لم تتوفر الحماية الكافية، يمكن أن تستخدم الجهات الفاعلة الخبيثة منافذUSB لحقن البرامج الخبيثة/APTS في أنظمة الترفية في الطيران مع عواقب وخيمه.

- **هجمات DDoS والروبوتات:**

قد نمت وازدادت شعبية هجمات الحرمان من الخدمة الموزعة تنفيذ مجموعة من أنشطة حقن البرامج الضارة. في مثل هذه الهجمات، يستخدم المتسللون روبوتات تعرض الشبكات للخطر لضبط حركة المرور الجوي وغيرها من الأنظمة المهمة (مثل التذاكرعبر الإنترنت الحجز) مع حركة

المرور، مما يؤدي إلى تعطل النظام الأساسي. قد يطلب المهاجمون أيضًا مبلغ فدية من السلطات لمنع تعطل إدارة االطيران والسيطرة عليها.

- **هجمات التشويش:**

يمكن أن يكون للهجوم عواقب وخيمة حيث يقوم المتسللون بتسوية دقة البيانات المقدمة لإدارة الطائرات، مثل السرعة والموقع والاتجاه والمطارات القريبة والطائرات الأخرى.[11]

- **الاختطاف عن بعد:**

العيوب الامنية في تكنولوجيات الاتصالات المستخدمة في الطيران، صناعة تمكن القراصنة للهجوم عن بعد/ التحكم عن بعد في أنظمة الطيران وعلى متن الطائرة التي[12] بدورها يمكن فتح بوابة للجهات الفاعلة الخبيثة مهاجمة أنظمة حرجة أخرى مثل الطيران أدوات التحكم، ونظم المحرك والوقود، وأجهزه إستقبال الملاحة، وأنظمه المراقبة، شاشات الطائرات، وغيرها.[13]

3.2.1. تصنيفات ودوافع المهاجمين:

يمكننا تصنيف المهاجمين المحتملين وفق معاييرعديدة:

- **موقع مكان المهاجم:**

عادة ما يتم اعتبار نوعين من المهاجمين، "الفئة الداخلية" وهم موظفو الشركات التي تنتج برمجيات التشغيل أو الذين يقومون بضمان الصيانة،

والنوع الثاني هم "الغرباء" الذين ليسوا موظفين بالشركات المتأثرة. كما يوجد فئة معينة اخرى وهي فئة المهاجمين الركاب على متن الطائرات

يمكن تقسيم الغرباء إلى فئات مختلفة، اعتمادًا على دوافعهم:

- **قراصنة المعلومات:**

هي فئة قراصنة المعلومات المعروفين في اللغة الإنجليزية باسم الهاكرز: يمكننا أيضًا تقسيم هذه الفئة إلى عائلتين، القبعات البيضاء الذين

يسعون الى البحث واكتشاف نقاط الضعف المؤدية إلى اختراق أنظمة التشغيل، ومن اجل هذا العمل، الكشف عن الثغرات الأمنية يقومون بالحصول على أموال من قبل الشركات التي تنتج الأنظمة (نتحدث إستغلال) هناك أيضا القبعات السوداء الذين يقومون بشكل عام باستغلال نقاط الضعف التي وجدوها أو التي قاموا باسترجاعها على الإنترنت مقابل المال. [14]

تسعى القبعات السوداء عمومًا الى تحقيق مكاسب مالية، لكن إذا لم يتم دفع فدية لهم بامكان هذه الاخيرة تهديد شركات الطيران وذلك بالتسبب في حادث أو حوادث خطيرة.

- **مجرمي الإنترنت:**

الذين هم في كثير من الأحيان عبارة منظمات مثل العصابات الحقيقية، مع تقسيم المهام بين مختلف الأعضاء هاته الاخيرة.

توجد هذه العصابات في العديد من البلدان التي توجد فيها لوائح قانونية غير مشددة كما هو الحال في فرنسا. والحافز الكبير لهاته الاخيرة هي المكاسب إضعاف المنافسة، وتشويه سمعة الشركات المنافسة لها في السوق، كما تستعملهم بعض الدول التي لا تريد أن يتم اكتشاف أصل بعض الهجمات ولاتريد ان تتهم فيها وهذا بموجب عقد ايضا.

هناك فئة من المهاجمين السيبرانيين المنظمين الذين يقومون باطلاق

هجمات منسقة ضد أهداف من اجل التعبيرعن معارضتها لبعض المشاريع أو بعض الشركات، وذلك لأسباب متنوعة للغاية كالدفاع عن البيئة (على سبيل المثال ضد بناء مطار جديد) أو الدفاع عن أسباب سياسية معينة. يطلق عليهم "المتسللين " هذه الفئة لاتهتم بالمكاسب المالية ولكنهم يقومون بالازعاج.

- **المحاربون عبر الإنترنت:**

هاته الفئة موجودة في بعض البلدان، عموما مع الوضع العسكري الحالي، وتستعد للحرب السيبيرانية المستقبلية. لديهم وسائل مالية كبيرة. منظمون في فرق حقيقية متعددة التخصصات والمتخصصة في مجالات معينة. يتم تكوين هاته الفئة خصيصا من اجل هذه المهام، ولا سيما المهام المسببة للدمار.[15]

- **الإرهابيين الالكترونيين:**

والذين يشبهون إلى حد ما المحاربين السيبرانيين، الذين يعملون بشكل عام بطريقة منسقة، والذين يهدفون الى افتعال الحوادث أو الحوادث الخطيرة.

لقد أصبح الإرهابيون يجدون صعوبة متزايدة في ركوب الطائرات بالأسلحة والمتفجرات ولهذا أصبح الخطر الموجود حاليا في إعادة تركيز أعمالهم الإجرامية على إرهاب الانترنت. هؤلاء الإرهابيون لديهم موارد مالية كبيرة، والتي تم الحصول عليها من بطريقة قانونية أو غير قانونية. ولحد الآن الإرهابيون الإلكترونيون لم يتسببوا بعد في تحطم طائرة.[16]

2.المحور الثاني: الجهود الدولية في مكافحة الجرائم السيبيرانية المهددة لأمن وسلامة الطيران المدني:

تتعدد الاليات والهيئات التي تعنى بامن وسلامة الطيران المدني على المستويات الدولية والاقليمية والوطنية كما ان الهجمات السيبيرانية اصبحت واقع معاش ة وهذا يظهر من خلال مختلف الهجمات التي وقعت على الطيران المدني، ومن اجل دراسة وافية لهذه النقاط ارتاينا تقسيم هذا المحور الى مايلي:

1.2.الهيئات الكفيلة بحفظ امن وسلامة الطيران المدني:

تتعد وتختلف الهيئات التي تحمي امن وسلامة الطيران المدني فنجد:

1.1.2.المنظمات الدولية:

من اهم المنظمات المدنية التي تعمل في مجال حماية الطيران المدني نجد:

- **الطيران المدني الدولي (الايكاو) :**

وكالة متخصصة تابعة للأمم المتحدة، أنشأتها دول في عام 1944 لتولي إدارة وتنظيم شؤون اتفاقية الطيران المدني الدولي (اتفاقية شيكاغو.)

وتعمل الإيكاو مع الدول الأعضاء في الاتفاقية وعددها 193 دولة ومع مجموعات قطاع الطيران للتوافق على القواعد والتوصيات الدولية[17] (SARPs) التي تخص الطيران المدني الدولي والسياسات الرامية إلى دعم قطاع طيران مدني يمتاز بالسلامة والكفاءة والأمن والإستدامة الاقتصادية والمسؤولية البيئية. وتستخدم الدول الأعضاء في الإيكاوهذه القواعد والتوصيات الدولية والسياسات لضمان تقيد عمليات الطيران المدني المحلية واللوائح التنظيمية لديها بالقواعد العالمية، ما يتيح بدوره التشغيل الآمن والموثوق لما يفوق 000 100 رحلة جوية يوميا ضمن الشبكة العالمية للطيران في كل مناطق العالم.

وبالإضافة إلى نشاطها الرئيسي في معالجة القواعد والتوصيات الدولية والسياسات التي يحرّكها التوافق بين دولها الأعضاء وقطاع الطيران.[18]

2.1.2. المنظمات الدولية الاقليمية:

من بين المنظمات الاقليمية التي تعنى بمكافحة الجرائم السيبيرانية لدينا:

- **المركز الاوروبي للامن السيبيراني في الطيران (ECCSA)**

المركز الاوروبي للامن السيبيراني في الطيران هي شراكة طوعية وتعاونية داخل مجتمع الطيران من أجل فهم مخاطر الأمن السيبراني الناشئة في مجال الطيران بشكل افضل ومن اجل توفير الدعم الجماعي في التعامل مع حوادث الأمن السيبيراني ومواطن الضعف والتفاعلات غير المصرح بها والتي يمكن أن تؤثر على مرونة القطاع وسلامته.

تعتبرالمشاركة في المركز الأوروبي للامن السيبيراني في الطيران طوعية وكذلك تبادل المعلومات، يجوز للمنظمات ذات الصلة بسلامة وأمن

الطيران المدني الأوروبي ان تتقدم بطلب للحصول على عضوية المركز الاوروبي للامن السيبيراني في الطيران، مع ضمان الايفاء بمعايير اختيار الأمان المطبقة[19].

3.1.2. الهيئات الوطنية

من اهم الهيئات الوطنية والمصنفة في اوائل الهيئات التي تعنى بالامن وسلامة الطيران المدني وهي:

- **الهيئة العامة للطيران المدني القطري (QCCA) :**

تعتبر الهيئة مؤسسة حكومية رسمية يعترف بها داخلياً وخارجياً تُعنى بشؤون الطيران المدني وتشارك في وضع السياسات المتعلقة به على المستويين الإقليمي والدولي من خلال إداراتها ووحداتها داخلياً والمنظمات والاتحادات التي تنتمي إليها خارجياً

تم انشاء الهيئة العامة للطيران المدني عام 2001 وفقاً للقانون رقم (16) لسنة 2001، وتعمل الهيئة على تطبيق أحكام قانون الطيران المدني رقم (15) لسنة 2002، وتم تعديل القانون في عامي 2008 و2011، وفقاً للمتطلبات والمستجدات الحاصلة في قطاع الطيران محلياً وإقليمياً وعالمياً. وللهيئة العامة[20]

للطيران المدني شخصية اعتبارية وموازنة ملحقة بموازنة وزارة المواصلات والاتصالات[21].

2.2 . جهود منظمة الطيران المدني الدولي و الهيئة العامة للطيران المدني القطير في محاربة الجرائم السيبيرانية:

لعبت منظمة الطيران المدني الدولي والهيئة العامة للطيران المدني القطري دورا هاما في حماية هذا القطاع من المهددات السيبيرانية و تتلخص اهم هذه الجهود فيما يلي:

1.2.2 **جهود منظمة الطيران المدني الدولي في مجال مكافحة التهديدات السيبيرانية:**

في أوائل السبعينات، نشرت الايكاو وثيقة أمنية، دليل لمساعدة الدول الأعضاء فيها علي اتخاذ تدابير لمنع الجريمة الغير مشروعة التداخل ، والتقليل من أثاره، والمعايير المعمول بها باعتماد الملحق 17من اتفاقية شيكاغو ، مما ينشئ ثقافة أمنية. ومع ذلك، فانه تم ترك التهديد الذي يشكله الأمن السيبراني دون معالجه حتى الاونه الاخيرة.

بدا برنامج التدقيق الامني مؤخرا مراجعه حسابات ضوابط الوصول والثغرات الامنية ذات الصلة في نظم تكنولوجيا المعلومات والاتصالات.[22]

وكانت هذه أول خطوه إلى الامام في تحديد المخاطر المحتملة في الأمن السيبراني. وعل مر السنين، وقد عززت الايكاو بفعالية المعايير والممارسات الموصي بها[23]

(SARPs) وتطورت الممارسات الجديدة الموصي بها فيما يتعلق بشبكة الحركة الجوية الأمان أيضا فرقه العمل الهندسية للإنترنت (IETF)، شركه الإنترنت للأسماء والأرقام المخصصة (ICANN)، الطيران الفيدرالي والمراقبة الاوروبية وفي ال2009، وبناء علي إيعاز من المؤتمر الأوروبي للطيران المدني، فريق الأمن الجوي إلى جانب الفريق العامل المعني بالاعمال[24]

الجديدة والتهديدات الناشئة، والنظر في التحديات التي يطرحها الأمن السيبراني؛ خرج مع[25] عدة توصيات، والتي تشمل على سبيل المثال لا الحصر تقييم المخاطر السيبيرانية وإدماج "عدم القدرة على التنبؤ" في قواعد البيانات القياسية على أساس مقترحات لجنة التدخل غير المشروع، التعديل الثاني عشر، وبناءً على توصيات فريق أمن الطيران، التعديل الرابع عشر، تم تطبيق الملحق 17 من يوليو 2011 ونوفمبر 2014 على التوالي.

الآن يتناول الفصل 4 من الملحق 17 التهديدات الإلكترونية .توصي بما يلي:

يجب أن تضع كل دولة متعاقدة تدابير لحماية المعلومات ونظم تكنولوجيا الاتصالات المستخدمة لأغراض الطيران المدني من التدخل الذي قد يعرض سلامة الطيران المدني للخطر[26] " .

على الرغم من أن هذا الحكم هو في طبيعة التوصية ، فإن الحاجة الملحة لمعالجة المخاوف المتعلقة بالأمن السيبراني قد تضطر الدول إلى اتخاذها الجهود المبذولة في هذا الاتجاه.[27]

- **بعض خطوات الايكاو في ترشيد الامن السيبراني**

ولقد بدا من الضروري ترشيد هذا الموضوع وعولمته من خلال مراعاة البعد الحكومي بالكامل. ثم أدى هذا العمل إلى اعتماد الجمعية 39 لمنظمة الطيران المدني الدولي في أكتوبر 2016 القرار A39-19 بشأن "الأمن السيبراني في الطيران المدني" ، وهو أول قرار للمنظمة مخصص بالكامل لهذا الموضوع. القرار A39-19 يضع المنظمة في نظام العمل ويشرف على العمل في فترة الثلاثية الجديدة 2017-2019 الذي يفتح. يمكن ذكر الخطوات التالية في هذا الصدد:

- ✓ **4-6 أبريل 2017:**

استضافت الايكاو ندوة بالشراكة مع دولة الإمارات العربية المتحدة في دبي. وانتهى بإصدار إعلان ينص على أن مسؤولية تخفيف مخاطر الإنترنت تقع على عاتق الدول، مع الدعوة إلى التعاون والتبادل بينها، وكذلك الاستخدام السلمي لقدرات الإنترنت.

- ✓ **صيف 2017:**

أنشأت الأمانة "مجموعة دراسة الأمانة حول الأمن السيبراني "(SSGC) من أجل استكشاف المنطقة ووضع برنامج عمل. هاته المجموعة التي اجتمعت بالفعل 5 مرات منذ اجتماعها الأول في أغسطس 2017 ، براسة نائب المدير المكلف بالأمن والهادف إلى أن يكون بمثابة "مركز تنسيق" لجميع أعمال

الايكاو المتعلقة بـ الأمن السيبراني. يجمع ما يقرب من عشرين خبيرا من الدول الأعضاء والصناعة ، ويتكون من عدة مجموعات تعمل في مواضيع محددة ، مثل الجوانب القانونية ، المطارات أو صلاحية الطائرات للطيران.

✓ **7 - 9 ماي 2018:**

سمحت قمة الايكاو في بوخارست لأوروبا وإفريقيا والشرق الأوسط بعنوان "الأمن السيبراني في الطيران المدني" بمزيد من العمل في هذا المجال.[28]

يقترح البيان المنشور تطوير إطار عمل منسق للأمن السيبراني في مجال الطيران المدني ، وتعزيز التعاون الإقليمي وتبادل المعلومات. كما أشار إلى الحاجة إلى الطيران المدني الدولي لتأمين استراتيجية عالمية ، تحت رعاية منظمة الطيران المدني الدولي.[29]

2.2.2. جهود الهيئة العامة للطيران المدني القطري (QCCA) :

أصدرت الهيئة العامة للطيران المدني بالتعاون مع قطاع شؤون الأمن السيبراني في وزارة المواصلات والاتصالات الإصدار الأول من "المبادئ التوجيهية للأمن السيبراني في مجال الطيران المدني"، والتي تضمنت المبادئ والمعايير الأمنية لحماية المناطق الحيوية في قطاع الطيران، بالإضافة إلى أفضل الممارسات المتبعة في الأمن الإلكتروني في هذا المجال.

وقالت الهيئة العامة للطيران في بيان، تلقت المنظمة نسخة منه، ان دولة قطر تعتبرأول دولة في منطقة الشرق الأوسط تقوم بإصدار مواد إرشادية تتركز على تطبيق معايير الأمن للتصدي والحد من التهديدات والهجمات الإلكترونية في قطاع الطيران المدني، والتي ستساهم في توعية جميع أصحاب المصلحة والعاملين في منظومة الطيران المدني في دولة قطر، وتوجيههم لإتباع أفضل الممارسات في مجال الأمن الإلكتروني.[30]

3.2. نماذج عن التهديدات السيبيرانية لامن وسلامة الطيران المدني:

هناك أمثلة عديدة على حوادث اختراق وقرصنة في قطاع الطيران المدني خلال السنوات الأخيرة، ومنها ما يلي :

العمليات التي قام بها القرصان المحترف إلكترونيًّا "كريس روبرت" لعشرات الرحلات الجوية، والذي اعتقلته السلطات الأمريكية في إبريل 2015، بعد "تغريدة" له نشرها لشرح خطوات قرصنته لطائرة "يونايتد إيرلاينز" التي كان مسافرًا على متنها إلى نيويورك. وفي التحقيقات التي تمت من قِبل مكتب التحقيقات الفيدراليFBI، اعترف "كريس" بحقيقة ما ارتكبه، وأعطى شرحًا[31] كاملا لعملية قرصنة الطائرات من خلال "الإيثرنت"؛ وهي تكنولوجيا تم اعتمادها كأساس في تنفيذ عمليات المراسلة في الكثير من الشبكات المحلية.

كما تعرضت ست منشآت سعودية، في نوفمبر 2016، لهجمات قراصنة إلكترونيين، وكان على رأسها الهيئة العامة للطيران المدني التي تنظم حركة الطيران السعودي.

واستهدفت الهجمات الإلكترونية تعطيل الخوادم والأجهزة في هذه المنشآت للتأثير على الخدمات المقدمة، وحاولت الاستيلاء على بيانات الأنظمة الحاسوبية وزرع البرمجيات الخبيثة[32].

الخاتمة:

تعد الهجمات السيبيرانية من اخطر الهجمات التي تهدد امن وسلامة الطيران المدني، وهذا بسبب ان صناعة الطيران المدني اصبحت في وقتنا الحالي تعتمد اعتمادا كبيرا ووثيقا على وسائل الاتصال الالكترونية وعلى نطاق واسع وفي كافة العمليات البرية والجوية وكذلك في ادارة الحركة الجوية والمطارات.

وتختلتف وتتنوع الهجمات السيبيرانية باختلاف أنواع ودوافع المهاجمين، ولهذا تظافرت جهود هيئات المجتمع الدولي، مثل منظمة الطيران المدني، والمركز الأوروبي للامن السيبيراني في الطيران، والهيئة العليا للطيران المدني

القطري، في مجابهة هذا النوع من التهديد، فقاموا بوضع خطط واستراتيجيات للتحكم والحد من هذه الظااهرة و الحفاظ على أمن وسلامة الطيران المدني.

ولهذا خلصنا الى مجموعة من النتائج والتوصيات من بينها:

النتائج:

1. الجرائم السيبيرانية في الطيران المدني جرائم ماسة بالأمن الالكتروني.
2. تختلف وتتنوع أنواع الهجمات السيبيرانية والمهاجمين السيبيرانين في مجال الطيران المدني.
3. تتعدد الهيئات التي تعنى بالحفاظ على أمن وسلامة الطيران المدني.
4. الهجمات السيبيرانية تكبد خسائر فادحة في مجال الطيران المدني.
5. تقلل هذه الجرائم من مصداقية وسمعة الطيران المدني.

التوصيات:

1. التوعية بمخاطر الجرائم السيبيرانية الماسة بقطاع الطيران المدني.
2. زيادة المؤتمرات التي تعنى بالأمن السيبيراني في مجال الطيران المدني.
3. إنشاء هيئات خاصة على مستوى كل دولة لمكافحةهذا النوع من الجرائم.
4. إيجاد قواعد قانونية للحد من هذه الهجمات وايجاد السبل الكفيلة بمكافحتها.

التهميش والاحالات:

[1] -Sensors (Basel), Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls, Published online 2018 Dec 21. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6339064/?fbclid=IwAR3XVplwrPwynDZvMB9M7PCDKy2tKuTB_wRcI2fY4YR8-2l4Z7Jq8fvjkoM, check it out on 04/11/2019, at 16:12 pm.

[2] - علي زياد العلى،المرتكزات النظرية في السياسات الدولية،دار الفجر للنشر والتوزيع، القاهرة، مصر، الطبعة الاولى، 2017، ص224.

[3] -علي زياد العلى،المرجع السابق، ص224.

[4] -المرجع نفسه، ص225.

[5] - tomamasso de zan, fabrizio d'amore, federica di camillo, the deffence of civilisation aire traffic system from cyber threats, document IAI 15/23 E, DECEMBER 2015, IAI2016, p9

[6]-المرجع نفسه، نفس الصفحة

[7] خالد بن مرزوق بن سراج العتيبي، الجوانب الاجرائية في الجرائم المعلوماتية:دراسة مقارنة، مكتبة القانون والاقتصاد،1433ه، المملكة العربية السعودية، الرياض، الطبعة الاولى 1435ه/2014, ص31

[8]- خالد بن مرزوق بن سراج العتيبي، المرجع السابق, ص31.

[9]- المرجع نفسه،ص32

[10]- - Civil Aviation Authority and Ministry of Transport & Communications، Aviation Cyber Security Guidelines، Issued On: April 2019، P13

[11]- Civil Aviation Authority and Ministry of Transport & Communications، Aviation Cyber Security Guidelines , rèfeèrence prècèdente, p13.

[12] - Civil Aviation Authority and Ministry of Transport & Communications، Aviation Cyber Security Guidelines , rèfeèrence prècèdente, p13.

[13]-المرجع نفسه، ص14 .

[14]- LES DOSSIER ,Cybermenaces visant le transport aerien , AAE DOSSIER N°4,Toulouse-France, p81

[15]- LES DOSSIER,rèfeèrence prècèdente, p81.

[16] -المرجع نفسه، ص82.

[17] ---موقع منظمة الطيران المدني الدولي، https://www.icao.int/about-icao/Pages/AR/default_AR.aspx، اطلع عليه يوم 2019/12/14، الساعة 13:14.

[18] --موقع منظمة الطيران المدني الدولي، https://www.icao.int/about-icao/Pages/AR/default_AR.aspx، اطلع عليه يوم 2019/12/14، الساعة 13:14.

[19] -موقع منظمة المركز الاوروبي للامن السيبيراني في الطيران، https://www.easa.europa.eu/eccsa/general-news?search=&fbclid=IwAR3I3S75mBq3CIP1RejNuftS4qYOsDWNZWVSWSGbtTKCTQW1tPPUZvVeNRE، اطلع عليه يوم 2019/12/29، الساعة 00:23.

[20] - موقع الهيئة العامة للطيران المدني القطري، https://www.caa.gov.qa/ar-qa/About%20CAA/Pages/About-CAA.aspx?fbclid=IwAR33mXb3_4nZFybRweuvmyB_c97sMDtFAW2uwQOmGEkRQ7wYrmEhoDaL-I4. اطلع عليه يوم 2019/12/31، الساعة 03:18.

[21] - موقع الهيئة العامة للطيران المدني القطري، https://www.caa.gov.qa/ar-qa/About%20CAA/Pages/About-CAA.aspx?fbclid=IwAR33mXb3_4nZFybRweuvmyB_c97sMDtFAW2uwQOmGEkRQ7wYrmEhoDaL-I4. اطلع عليه يوم 2020/01/01، الساعة 06:14.

[22]- cyber security in civil aviation, july 2015, for EALA prize 2015, p7

[23] -cyber security in civil aviation, rèfeèrence prècèdente, p7

[24] - المرجع نفسه,ص9

[25]- deepeka jayakodi, rèfeèrence prècèdente,p9.

[26] - المرجع نفسه،ص 10

[27]- المرجع نفسه،ص11

[28] - موقع منظمة الطيران المدني الدولية https://oaci.delegfrance.org/Dossier-Cybersecurite-et-transport-aerien?fbclid=IwAR0JlYJlGHv99znHGIoyvYRO-1hCZaG335I-hNH_kEXfp9RkQQ_PvqVM7og ، اطلع عليه يوم 2019,/12/26 الساعة 14:07

[29] - موقع منظمة الطيران المدني الدولية https://oaci.delegfrance.org/Dossier-Cybersecurite-et-transport-aerien?fbclid=IwAR0JlYJlGHv99znHGIoyvYRO-

1hCZaG335I-hNH_kEXfp9RkQQ_PvqVM7og ، اطلع عليه يوم 2019,/12/27 الساعة 15:19.

[30] -موقع المنظمة العربية للطيران المدني، https://acao.org.ma/news_tayaran.php?id=66&fbclid=IwAR0g7BDF4R9r2faT3blFzKZZzlPQ8fbV0j6nVwFlPnK18CFp3yjZr1pfvdY، اطلع عليه يوم 2020/01/05، الساعة 08:05.

[31] - محمد عزت هلال، تهديدات الامن الالكتروني في قطاع الطيران المدني، الخميس 25 ماي 2017، https://futureuae.com/m/Mainpage/Item/2827، اطلع عليه يوم2019/12/03، الساعة 14:25.

[32]- محمد عزت هلال، تهديدات الامن الالكتروني في قطاع الطيران المدني، الخميس 25 ماي 2017، https://futureuae.com/m/Mainpage/Item/2827، اطلع عليه يوم2019/12/05، الساعة 02:36.

قائمة المراجع:

المؤلفات باللغة العربية:

1. العتيبي،خالد بن مرزوق بن سراج،1435ه/2014,الجوانب الاجرائية في الجرائم المعلوماتية:دراسة مقارنة، المملكة العربية السعودية، الرياض، الطبعة الاولى، مكتبة القانون والاقتصاد،1433ه.

2. فكري،ايمن عبد الله، 1435ه/2014، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والاجنبية، المملكة العربية السعودية، الرياض، الطبعة الاولى, مكتبة القانون والاقتصاد،1433ه.

3. علي زياد العلى، 2017، المرتكزات النظرية في السياسات الدولية، دار الفجر للنشر والتوزيع، القاهرة، مصر، الطبعة الاولى.

مواقع الانترنيت:

1. محمد عزت هلال، تهديدات الامن الالكتروني في قطاع الطيران المدني، الخميس 25 ماي 2017، https://futureuae.com/m/Mainpage/Item/2827.

2. موقع منظمة المركز الاوروبي للامن السيبيراني في الطيران ، https://www.easa.europa.eu/eccsa/general-

news?search=&fbclid=IwAR3I3S75mBq3CIP1RejNuftS4qYOsDWNZW VSWSGbtTKCTQW1tPPUZvVeNRE.

3. موقع المنظمة العربية للطيران المدني، https://acao.org.ma/news_tayaran.php?id=66&fbclid=IwAR0g7BDF4R9r 2faT3blFzKZZzlPQ8fbV0j6nVwFlPnK18CFp3yjZr1pfvdY، .

4. موقع منظمة الطيران المدني الدولية https://oaci.delegfrance.org/Dossier-Cybersecurite-et-transport-aerien?fbclid=IwAR0JlYJlGHv99znHGIoyvYRO-1hCZaG335I-hNH_kEXfp9RkQQ_PvqVM7og .

5. موقع الهيئة العامة للطيران المدني قطر، https://www.caa.gov.qa/ar-qa?fbclid=IwAR1suh5Xq0PN24QdNE9EE3QFbg8j073AFRsScowf5i2gE 7j8niTgrJtxAu4.

6. Sensors (Basel), Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls, Published online 2018 Dec 21. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6339064/?fbclid=IwAR3XVplwrPwynDZvMB9M7PCDKy2tKuTB_wRcI2fY4YR8-2l4Z7Jq8fvjkoM..

المؤلفات باللغة الاجنبية:

1. Civil Aviation Authority and Ministry of Transport & Communications,2019, Aviation Cyber Security Guidelines.
2. LES DOSSIER,2019, Cybermenaces visant le transport aerien , AAE DOSSIER N°4,Toulouse-France.
3. tomamasso de zan, fabrizio d'amore, federica di camillo,2016, the deffence of civilisation aire traffic system from cyber threats, document IAI 15/23 E, DECEMBER 2015, IAI2016.

المقالات باللغة الاجنبية:

1. deepeka jayakodi, july 2015,cyber security in civil aviation, for EALA prize 2015.