

التعاون الأمني في جنوب شرق آسيا في مواجهة تهديدات الأمن السيبراني

Security cooperation in Southeast Asia in countering cyber security threats

حميدة لحمر^{1*}، جامعة جيجل، (الجزائر)، hamida.lahmer@univ-jijel.dz

فريدة حموم²، جامعة جيجل، (الجزائر)، f.hamoum@gmail.com

تاريخ قبول المقال: 20-05-2021

تاريخ إرسال المقال: 01-05-2021

الملخص:

تحاول هذه الورقة معالجة الطريقة التي تنتظر بها دول جنوب شرق آسيا لتهديدات الأمن السيبراني، ومدى جاهزية هذه الدول إلكترونيا لمواجهة هذه التهديدات، من خلال التطرق للوضع الأمني السيبراني فيها، وما اتخذته من إجراءات ومبادرات تعاونية، وقد خلصت الورقة البحثية إلى نتيجة مؤداها أن دول الآسيان رغم وعيها بخطورة التهديدات السيبرانية، واعترافها بضرورة التعاون الأمني السيبراني إلا أنها لا تزال في مراحلها الأولى من التعاون، نظرا لتباين قدراتها السيبرانية وأولوياتها الأمنية، لذلك ينبغي عليها أولا بناء قدراتها الإلكترونية الفردية (الدولانية) قبل الجماعية، من أجل ضمان فعالية التعاون.

الكلمات المفتاحية: التعاون الأمني، الأمن السيبراني، تهديدات الأمن السيبراني، جنوب شرق آسيا.

Abstract: This paper tries to treat the way in which Southeast Asian countries have viewed cyber security threats, and the extent to which these countries are electronically prepared to confront these threats, by addressing the cyber security situation in them, and the measures and cooperative initiatives they have taken. Despite its awareness of the seriousness of cyber threats, and recognition of the necessity for cyber security cooperation, it is still in its early stages of cooperation, given its varied cyber capabilities and security priorities, so it should first, its individual (state) cyber capabilities were created before the collective, in order to ensure effective cooperation.

Key words: security cooperation, cyber security, cyber security threats, south East Asia.

*حميدة لحمر

مقدمة:

يعكس تزايد الاعتماد على الفضاء الإلكتروني في مختلف مجالات الحياة ظاهرة مزدوجة التأثير؛ فقد ساهم الفضاء الرقمي في تسهيل التفاعل بين المجتمعات والشعوب، واختصر الوقت والجهد، وقلص المسافات وقلل من التكاليف بين مختلف الفواعل الدولية، لكنه أدى بنفس القدر إلى تنامي التحديات والتهديدات الأمنية في صور جديدة للتنافس والتصارع، وبآليات وأساليب مختلفة، وبدرجات جاهزية وتحكم متباينة، الأمر الذي جعل من مراجعة الآليات المنظمة والضابطة للتفاعل الدولي في الفضاء السيبراني ضرورة ملحة بغرض التكيف مع الواقع الجديد.

يحظى موضوع الأمن الإلكتروني بأهمية واهتمام واسع النطاق على المستويين الأكاديمي والعملية لما ينطوي عليه من ارتباطات وتشابكات جعلت منه أحد أبعاد القوة والأمن على حد سواء، بالشكل الذي أسس لنمط جديد من التعاملات والتفاعلات على مستوى العلاقات الدولية سواء في فترات الحرب أو في فترات السلم. كما أن الآسيان التي تأسست سنة 1967 تحظى باهتمام متزايد من قبل في إطار الدراسات الإقليمية لما تعرفه من تطور مستمر وديناميكية متسارعة على المستوى الاقتصادي كما على المستوى السياسي والأمني.

تهدف بذلك هذه الورقة البحثية لمعرفة مدى قدرة دول جنوب شرق آسيا كدول تشهد تطورا اقتصاديا متباينا، استطاعت أن تشكل كيانا إقليميا فاعلا في العلاقات الدولية على التكيف مع ضرورات العصر الرقمي وسبل الاستفادة منه، انطلاقا من البحث في الآليات والمبادرات المستحدثة لمواجهة هذه التهديدات، بما يسمح لنا بالتعرف على مدى نضج الرؤية المشتركة لدول الآسيان إزاء الأمن السيبراني؛ إذ تعتبر منطقة جنوب شرق آسيا كمنطقة حديثة العهد بالاندماج التكنولوجي من أكثر المناطق التي تشهد تصاعدا مستمرا لتهديدات الأمن السيبراني تزامنا مع تزايد عدد مستخدمي الانترنت؛ الأمر الذي أضاف تحديا جديدا للآسيان كتكتل اقتصادي، ومركب أمن إقليمي، ومشروع لبناء جماعة أمنية آسيانية، وهو ما يدفعنا للتساؤل عن مدى تطور الاستجابة التعاونية لدول جنوب شرق آسيا في مواجهة هذه التهديدات وذلك انطلاقا من الإشكالية التالية:

ما مدى جاهزية دول جنوب شرق آسيا إلكترونيا للتعاون الأمني في مواجهة تهديدات الأمن

السيبراني؟

يندرج تحت هذه الإشكالية الأسئلة الفرعية التالية:

- ما هي أهم تهديدات أمن الفضاء السيبراني؟

- كيف يمكن توصيف الواقع الأمني الإلكتروني لدول الآسيان؟
- فيم تتمثل أهم المبادرات التعاونية لدول الآسيان في مواجهة تهديدات الأمن السيبراني؟
- من أجل الإجابة على هذه التساؤلات نقترح الفرضيات التالية:
الفرضية الرئيسية:
يحظى أمن الفضاء السيبراني والتهديدات الإلكترونية باهتمام متزايد في مسار التعاون الأمني لدول جنوب شرق آسيا.
الفرضيات الفرعية:
1- يعتبر الارهاب الإلكتروني من أهم تهديدات أمن الفضاء السيبراني.
2- يجمع الواقع الأمني الإلكتروني لدول الآسيان بين التطور التكنولوجي المتسارع والانتشار المتزايد للتهديدات الإلكترونية.
3- تتخبط دول الآسيان ضمن تفاعلات تعاونية داخلية وخارجية من أجل مواجهة تهديدات أمن الفضاء السيبراني.
منهجية الدراسة: اعتمدت الدراسة لمعالجة هذه الإشكالية على المنهج التحليلي من خلال تحليل التطورات الحاصلة في دول الآسيان على مستوى التطور التكنولوجي، وطريقة تعاظم دول الآسيان مع تهديداته الأمنية، المنهج الاستقرائي من خلال قراءة المعطيات والبيانات التي تم جمعها حول التعاون السيبراني في المنطقة، مما يسمح لنا بتشكيل رؤية حول مدى نضج المسار التعاوني في هذا المجال، بالإضافة للاقترب النظمي الذي تمت الاستعانة به من خلال دراسة التفاعل بين الآسيان كوحدة تحليل ممثلة للمستوى الإقليمي مع متغيرات البيئة الداخلية والخارجية كمستويين جزئي وكلي.
قسمت الدراسة إلى ثلاثة محاور كالاتي:
المحور الأول: تهديدات أمن الفضاء السيبراني
المحور الثاني: تهديدات الأمن السيبراني و الجاهزية الإلكترونية لدول الآسيان
المحور الثالث: مبادرات الآسيان التعاونية لتحقيق الأمن السيبراني

المحور الأول: تهديدات أمن الفضاء السيبراني

يتم التطرق في هذا المحور لأهم ما يعترض الدول والمجتمعات من تهديدات إلكترونية تستدعي اللجوء للتعاون من أجل التصدي لها.

يضم الفضاء السيبراني حزمة متنوعة من التهديدات الإلكترونية، بعضها يطل الاقتصاد، وبعضها يهدد الأنظمة السياسية والاستراتيجيات العسكرية، والبعض الآخر يهدد المجتمعات وهويتها وثقافتها، وعليه سيتم التطرق لأهم هذه التهديدات فيما يلي:

أولاً: الإرهاب الإلكتروني

سيتم التطرق في هذا العنصر للتطور الذي لحق بالإرهاب كمفهوم وكظاهرة، من خلال التركيز على ما أضافته الثورة التكنولوجية من متغيرات.

فقد كان لتطور شبكات الاتصال والمعلومات دوراً في تحول الإرهاب من تهديد محلي إلى تهديد عالمي من حيث النشاط والخطط والتمويل، ذلك أن الجماعات الإرهابية اليوم تضم أفراداً من جنسيات مختلفة، وعلى درجة عالية من الكفاءة التكنولوجية، كما أصبحت التكنولوجيا من الوسائل الداعمة للعمل الإرهابي ومحركاً لديناميكيته وسهولة انتشاره بما أتاحته من شبكة عالمية للاتصالات والتعبئة والتمويل، استفادت منها الجماعات الإرهابية في زيادة قدرتها على التجنيد، والتواصل مع بعضها البعض، ومكنتها من تطوير أسلحتها حتى باتت تهدد باستخدام أسلحة الدمار الشامل، مما أدى إلى تغييرات على مستوى التنظيم والمبادئ والتقنية المستخدمة والاستراتيجية المتبعة والفواعل المؤثرة.¹

ينبغي الإشارة إلى أن الإرهاب الإلكتروني ما هو إلا نسخة مطورة عن الإرهاب التقليدي نظراً لتوافر وسائل وآليات متطورة لتنفيذ العمليات الإرهابية، لذلك سنعرض لتطور الإرهاب الإلكتروني على المستويين المفاهيمي والامبريقي.

1- على مستوى المفهوم:

جرت العادة على تعريف الإرهاب على أنه الاستخدام غير المشروع للقوة والعنف ضد الأشخاص أو الممتلكات لترويع أو إجبار الحكومات أو الناس العاديين أو أي جزء منهم من أجل تحقيق أهداف اجتماعية أو سياسية، أما الإرهاب الإلكتروني فظهر أول مرة في فترة الثمانينات في دراسة "باري كولن" Barry Kollin أقر فيها بصعوبة تعريف الظاهرة بالنظر لتشعبها وتعقدها، ففي عام 1980 كان المصطلح يشير إلى تلك الهجمات التي يستخدم فيها الكمبيوتر ضد اقتصاد وحكومة الولايات المتحدة، ثم اتسع المفهوم وعمم مع انتشار أدوات تكنولوجيا الاتصال في إطار ظهور مجتمع المعلومات العالمي

ليصبح دالا على استخدام الفضاء الإلكتروني لإلحاق الضرر أو تعطيل البنية التحتية كالمواصلات والمنشآت الطاقوية والمؤسسات الحكومية، من أجل تحقيق أهداف سياسية.

وقد عرفته دينينغ دورتي D.Denning على أنه: «هجمات غير قانونية وتهديدات بالهجوم ضد الحاسبات والشبكات والمعلومات المخزنة وذلك لتخويف أو إجبار حكومة أو شعبها بهدف تعزيز أهداف سياسية أو اجتماعية، ولكي يكون إرهابا يجب أن ينتج عنه عنف اتجاه الأفراد أو الممتلكات أو على الأقل التسبب بضرر ينتج عنه توليد الخوف». أما "جيمس لويس" من مركز الدراسات الاستراتيجية والدولية فيعرفه على أنه: «استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القومية (مثل الطاقة، والمواصلات وعمليات الحكومة أو إكراه أو ترهيب الحكومة أو السكان المدنيين)².

كما عرفت موسوعة المعرفة الإرهاب الإلكتروني بأنه: «استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية»³، فمجمال التعاريف ترى أن الإرهاب الإلكتروني يستغل الفضاء السيبراني أو إحدى مكوناته لتنفيذ هجماتهم وفي ممارستهم للعنف الغير مشروع.

2- على المستوى الإمبريقي:

كان ظهور الفضاء الإلكتروني بشكل علني في الصراع الدولي في التوتر بين روسيا واستونيا في ماي 2007 وأوت 2008 خلال الحرب بين جورجيا وروسيا، مما أثار جدلا حول التحديات التي يثيرها الفضاء الإلكتروني والتي تتمحور أساسا حول:⁴

- 1- غموض دور الفاعلين في الهجمات الإرهابية.
- 2- تجاوز الحدود التقليدية للدول؛ حيث قد يأتي الهجوم من أي مكان وفي أي وقت بالنظر لسرعته وانخفاض كلفته.

3- يعتمد على آليات ذاتية الحركة وتحدث أضرار كبيرة على مستويات عدة.

4- يتيح الفضاء الإلكتروني الفرصة لاتساع المشاركين في الصراع.

ورغم كل هذه الأضرار، إلا أن القانون الدولي قد ركز على تجريم ومنع استخدام القوة في العلاقات الدولية. مما شكل فجوة بين الأطر القانونية الدولية وهجمات الفضاء الإلكتروني، حتى أننا لا نجد اتفاقية دولية تتناول الفضاء الإلكتروني بشكل مباشر رغم أن هذا الأخير يعبر عن استخدام نمط آخر من القوة في العلاقات الدولية.

ثانيا: الجريمة الالكترونية:

يتكون هذا المصطلح من كلمتين هما: الجريمة التي تدل على كل الأفعال الغير مشروعة، والإلكترونية التي تدل على الفضاء الالكتروني -مكان حدوث الجريمة-، فالجرائم الالكترونية تدل على المخالفات التي ترتكب ضد الأفراد والمجموعات من الافراد بدافع الجريمة قصد إيذاء سمعة الضحية أو أذيته ماديا أو عقليا بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصالات مثل الانترنت (كغرف الدردشة والبريد الالكتروني، والهاتف). ويتمثل الهدف من الجريمة الالكترونية في تحقيق أهداف شخصية أو مكاسب مالية أو ضرر هوياتي وغيرها.⁵

تتعدد أشكال الجريمة الالكترونية بالنظر لما يوفره الفضاء السيبراني من فرص تمكن المجرمين من تصفح الانترنت وارتكاب مختلف الجرائم مثل القرصنة، والاحتيال، وتخريب الحواسيب وسرقة المعلومات وغيرها من صور الجريمة، مستغلين بذلك الخصائص الفريدة للفضاء السيبراني.⁶

ثالثا: حرب المعلومات (الحرب الالكترونية)

يستخدم هذا المصطلح للتعبير عن استخدام نظم المعلومات، لاستغلال وتدمير وتعطيل معلومات الخصم وعملياته المبنية على المعلومات، ونظم المعلومات، من قبل الخصم لإحراز السبق، والتقدم على نظمه العسكرية والاقتصادية. مما يعني أن الحرب الالكترونية تنقسم إلى شقين: شق هجومي وشق دفاعي، وكلاهما يتطلب تقولا تكنولوجيا لنجاحه.

من جهة أخرى يرى واين وارثو Wayne Wartow أن حرب المعلومات تشن على ثلاث مستويات هي:

- 1- حرب المعلومات الشخصية: تلك التي تستهدف خصوصية الأفراد.
- 2- حرب المعلومات بين الشركات والمؤسسات، وذلك في إطار المنافسة الاقتصادية بهدف تعطيل المنافس.
- 3- حرب المعلومات العالمية بين الدول أو بين دول معينة والقوى الاقتصادية العالمية، خاصة في حالة وجود عداوة بينهما.⁷

وتشير المصادر إلى أن بدايات أساليب الحرب الإلكترونية تعود إلى عام 1905 خلال الحرب الروسية اليابانية في معركة Tsushima، عندما كانت سفن الاستطلاع اليابانية تراقب الأسطول الروسي وترسل ما تم جمعه من معلومات إلى القيادة اليابانية الرئيسية عبر الراديو، ثم ما كان خلال الحرب العالمية الأولى من استعمال واسع لأجهزة الاتصال وأجهزة نقل معلومات الاستطلاع؛ إذ استطاعت سفن انجليزية أن ترسل معلومات عن تحرك بعض القطع الحربية الألمانية في البحر المتوسط عام 1914، وعمليات التشويش التي اتخذها الألمان تجاه ذلك كأسلوب للحماية والدفاع، إلا أن البداية الحقيقية

لاستخدام أجهزة الحرب الالكترونية فكانت في الحرب العالمية الثانية عام 1939 من خلال "تقاطع موجات التشويش فوق الهدف" التي استخدمها الألمان من أجل قصف المدن الإنجليزية.⁸ وقد توالى بعد ذلك استخدامات كل ما يتم تطويره تكنولوجيا في إدارة العلاقات الدولية سواء في فترات الحرب أو السلم من أجل تحقيق أهداف استراتيجية سواء عن طريق التأثير أو السيطرة على كل العناصر السياسية والاقتصادية والعسكرية والمعلوماتية عبر شبكة الانترنت، مما يعني أن الحرب الالكترونية في المجال العسكري مثلاً لا تستدعي الدبابات والجيوش، بل تختفي فيها المدافع والصواريخ وتنتقد الحواسيب للخطوط الأمامية، وكذلك الأمر بالنسبة للمجال الاقتصادي؛ أين يكون نشر إشاعة حول شركة ما كفيلاً بتكليفها خسائر كبيرة أو حتى تعريضها للإفلاس. لذلك يمكن القول بأن العلاقة بين حرب المعلومات والإرهاب الإلكتروني تتضح من خلال استخدام الإرهابيين لحرب المعلومات كأداة لتنفيذ أهدافهم.⁹

لقد أحدث الفضاء الرقمي أربع اتجاهات رئيسية من التغيرات، دفعت باتجاه المطالبة بالتدخلات الرسمية للحكومات من أجل حوكمة استخدام الانترنت وهي كالتالي:

- 1- الارتفاع المستمر في استخدام الانترنت، والتوسع في أشكال هذا الاستخدام.
- 2- إدراك الحكومات لآثار الأمانة للثغرات السيبرانية على أمنها القومي.
- 3- المشاركة اليومية للمواطنين واندماجهم في النشاطات السيبرانية اليومية.
- 4- اتساع الفجوة بين التطور التكنولوجي، وطبيعة استراتيجيات مواجهة التهديدات الناشئة.¹⁰

المحور الثاني: تهديدات الأمن السيبراني والجاهزية الالكترونية لدول الأسيان:

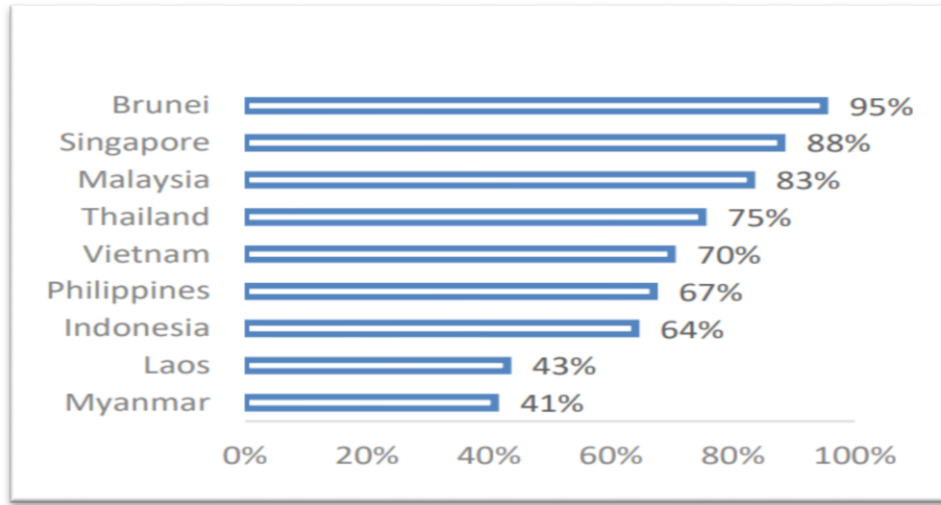
سيتم التطرق في هذا المحور أولاً لأهم تهديدات الأمن السيبراني، وثانياً للجاهزية الالكترونية لدول الأسيان.

أولاً: تهديدات الأمن السيبراني في دول الأسيان

إن منطقة جنوب شرق آسيا باعتبارها حديثة العهد مع التطور التكنولوجي، تعرف صورة مزدوجة من تبعات الولوج للعالم الرقمي؛ فمن جهة تخطو خطوات سريعة باتجاه التمكن من التكنولوجيا، ومن جهة أخرى تعرف انتشاراً واسعاً لمختلف جرائم الانترنت، فقد بلغ متوسط معدل انتشار الانترنت في جنوب شرق آسيا وفقاً للتقرير الرقمي العالمي لعام 2020 حوالي 66%، فقد شهدت المنطقة انتشاراً سريعاً خلال السنوات القليلة الماضية كما سيتضح في الشكل التالي، (نسب انتشار الانترنت في دول جنوب شرق آسيا)، إلا أن هذا الانتشار غير متماثل في كافة دول المجموعة؛ حيث تشهد إندونيسيا وكمبوديا أعلى

معدل نمو في المنطقة، إذ سجلنا على التوالي: 17%، 15%، أما بالنسبة للمستخدمين فيقضي المستخدمون في الفلبين وتايلاند أكبر قدر ممكن من الوقت يوميا والذي قدر بـ 9 إلى 10 ساعات يوميا.¹¹

الشكل 02: انتشار الانترنت في دول جنوب شرق آسيا:



المصدر: Interpol, Asean cyber threat assessment 2021 - key cyber threat trends Outlook from the Asean cyber crime Operations desk, 2021. p 11. at: www.interpol.int: 10/03/2021.

تشهد إذن منطقة جنوب شرق آسيا نموا هائلا في قطاع التكنولوجيا الرقمية خاصة منها التكنولوجيا المالية، والتجارة الالكترونية، مما جعلها من أكثر الأسواق تنافسية في العالم. وبالتوازي مع هذا التطور السريع شهدت المنطقة ظهور عدد كبير من التهديدات السيبرانية التي قد تحد من الإمكانيات الرقمية لدول الآسيان.¹²

كما تتعرض في ذات الوقت للهجمات الالكترونية بوتيرة متصاعدة نتيجة زيادة التجارة الالكترونية، وتدفقات رؤوس الأموال الكترونيا بين الدول الأعضاء؛ حيث تشير التقديرات إلى أن أكبر 1000 شركة في الآسيان معرضة لخسارة 750 بليون دولار بسبب التهديدات الالكترونية، مما سيعرقل تنفيذ الآسيان لأجندة الاقتصاد الرقمي التي أصبحت من أولويات الآسيان، فهذه ماليزيا قد بلغت عن 6800 حادث أمن إلكتروني اعتبارا من جويلية 2015، وفي سنة 2016 تم الإبلاغ عن اختراقات من أكثر من 2100 هيئة حكومية، إذ طالت الهجمات الإلكترونية حوالي 80%، أما إندونيسيا فقد أصبحت الدولة الأكثر عرضة للتهديدات الالكترونية؛ حيث تم تشويه أكثر من 12 ألف موقعا حكوميا عام 2013، فالتهديدات

السيبرانية تعرقل تنفيذ الآسيان لأجندة الاقتصاد الرقمي التي أصبحت من أولويات وقد تراوحت التهديدات الإلكترونية في المنطقة بين جرائم إلكترونية، وعمليات تجسس، وإرهاب إلكتروني، وقرصنة إلكترونية نورد أهمها فيما يلي:

1/ الجريمة الإلكترونية

كلفّت الجرائم الإلكترونية دول الآسيان في الفترة الممتدة من 2007 إلى 2012 ما يقارب 90 مليون دولار أمريكي، 30% منها ضد الأفراد، و70% منها ضد مؤسسات الدول، وتكلف الجريمة الإلكترونية إندونيسيا 2.7 بليون دولار سنوياً، بينما سجلت سنغافورة أعلى الخسائر الفردية جراء الجرائم الإلكترونية في العالم سنة 2013 والتي قدرت بـ 1158 دولار أمريكي.¹³

2/ القرصنة الإلكترونية

تعتبر القرصنة الإلكترونية هي الأخرى تهديدا كبيرا للأمن السيبراني في الآسيان نظرا لاعتماد آليات أمن تقليدية للبرامج؛ حيث بلغ معدل القرصنة في كمبوديا أكثر من 95%، تليها فيتنام وإندونيسيا بنسبة 80%، وتشير التقديرات إلى أن المستهلكين الإقليميين سينفقون 10.8 مليون دولار للتعامل مع قضايا البرمجيات الخبيثة المتعلقة بالبرامج المقرصنة، ففي فيتنام تم تسجيل 280000 هجوم إلكتروني في مدينة هوشي منه عام 2014، أي ما نسبته 300%، الأمر الذي جعل تقريراً صادراً عن Asia financial lines تابعة لـALG يحذر من أن فيتنام تحتل المرتبة الثالثة في قائمة الدول التي تحتوي أكثر التطبيقات المصابة بالفيروسات التي تم تنزيلها لنظام التشغيل Android، لتتكبد فيتنام خسائر سنوية تقارب 380 مليون دولار أمريكي.¹⁴

3/ الارهاب الإلكتروني

تم استخدام الفضاء الإلكتروني من قبل الجماعات الإرهابية لشن هجماتها وتشويه مواقع الانترنت، ونشر الدعايات الدينية والمتطرفة وإلحاق الضرر بالخدمات والأعمال التجارية، ففي ماليزيا قامت مجموعة من القراصنة ذات الصلة بتنظيم داعش تسمى Anon Chost باختراق حسابات Facebook و Twitter الخاصة بالشرطة الملكية الماليزية، كما تمكنت مجموعة القرصنة CyberCaliphate من اختراق موقع الخطوط الجوية الماليزية في جانفي 2015 مما عطل موقعها الإلكتروني. لقد كشفت الانترنت عما يقارب 9000 برنامجاً ضاراً، ومئات البرامج المخترقة في ثمانية دول من جنوب شرق آسيا، والتي تشمل عائلات البرامج الضارة التي تستهدف المؤسسات المالية، نشر برامج الفدية، توزيع البريد العشوائي وغيرها.¹⁵

ثانيا: الجاهزية الالكترونية لدول الآسيان:

سيتم التطرق في هذا العنصر لمختلف المبادرات التعاونية لدول الآسيان سواء على المستوى الدولي، أو الإقليمي أو العالمي، لكن قبل ذلك سيتم التطرق لمستوى جاهزية دول الآسيان إلكترونيا؛ حيث تتباين القدرات السيبرانية بين الدول المتقدمة نسبيا مثل سنغافورة وماليزيا وإندونيسيا ذات المواقف الفعالة لبلوغ هدفها بشأن تجسيد الاقتصاد الرقمي، وبين الدول النامية مثل كمبوديا ولاوس التي لا تعطي أهمية كبيرة للمجال الإلكتروني، لذلك أشار تقرير AT Kearney إلى أن منطقة جنوب شرق آسيا يجب أن تنفق ما يعادل 171 بليون دولار أمريكي بشكل جماعي بين عامي 2017/2025، من أجل تحقيق الحصانة المطلوبة ضد التهديدات الالكترونية¹⁶

تشهد دول الرابطة من جهة أخرى مستويات مرتفعة من عمليات الاختراق الإلكتروني كما سيوضحه الجدول التالي:

الجدول رقم 01: اختراقات الإنترنت في دول الآسيان:

الرقم	الدولة	عدد السكان	مستخدمو الإنترنت	نسبة اختراق الإنترنت (%)
1	بروناي	395027	318900	81%
2	سنغافورة	4701069	3658400	78%
3	ماليزيا	26160256	16902600	65%
4	الفلبين	99900177	29700000	30%
5	فيتنام	89571130	24269083	27%
6	تايلاند	66404688	17486400	26%
7	إندونيسيا	242968342	30000000	12%
8	ج. لاوس. ش	6993767	527400	8%
9	كامبوديا	173675	13800000	1.3%
10	ميانمار	110000	53414374	0.2%
	الآسيان	123146458	604308830	20(%)

المصدر: Krisman Khanisa, "A Secure connections: finding the forme of Asean cyber Security coopération", **journal of Asean studies**. vol.1, N° 1, 2013, p 44. At: <https://n9.cl/lppf>: 10/03/2021.

لقد أشارت التقديرات إلى أن دول الآسيان تتكبد خسائر كبيرة الجرائم الالكترونية، فإندونيسيا تخسر 2.7 مليار دولار سنويا جراء جرائم الانترنت، وبلغ نصيب الفرد السنغافوري من الخسائر بسبب الجرائم الالكترونية 1.158 دولار أمريكي، كما أنه وفقا لمركز آسيا والمحيط الهادي للمخاطر قد تمت سرقة بيانات شخصية لـ 850 شخصا عبر الانترنت، وفي أكتوبر 2018 كانت هناك أكثر من 46 مليون سرقة وتسريب لبيانات المشتركين في الهاتف المحمول في ماليزيا. أما بروناي فقد سجل فيها فريق الاستجابة للطوارئ الحاسوبية 2143 BruCert هجوما على أمنها السيبراني سنة 2018، بينما كانت شركة Toyota Motor Corporation ضحية لإصدار سلسلة من خروقات البيانات.¹⁷

كل هذا إنما ينم عن ضعف في حماية الفضاء الالكتروني، مما يجعل من التعاون الدولي أمرا ضروريا لضمان الأمن السيبراني، لذلك حاولت دول جنوب شرق آسيا تحقيق ذلك من خلال العديد من المبادرات في مستويات عدة.

المحور الثالث: مبادرات الآسيان التعاونية لتحقيق الأمن السيبراني

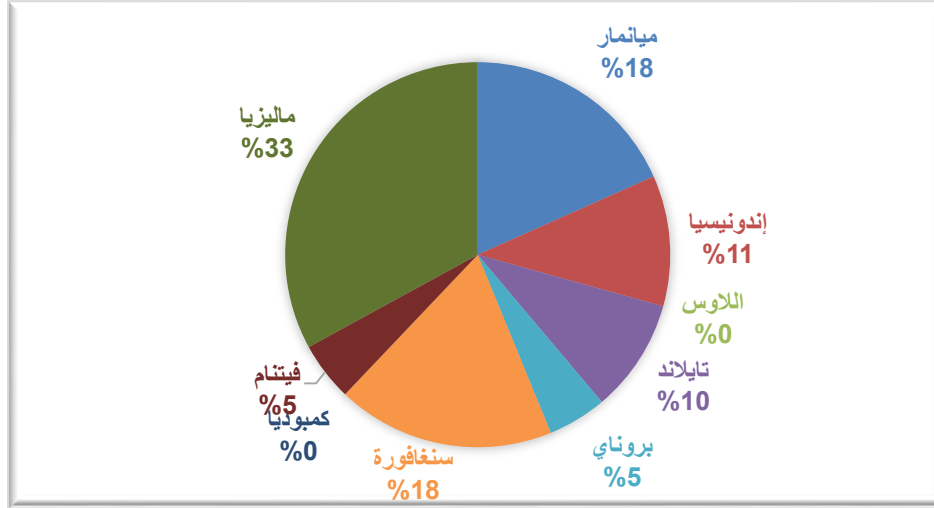
سيخصص هذا المحور لأهم ما تبدله دول جنوب شرق آسيا من جهود من أجل التصدي للتهديدات الالكترونية سواء على المستوى الداخلي أو على المستوى الخارجي.

أولا: المبادرات داخل دول الآسيان

1- برنامج البحث والابتكار

يعتبر البرنامج أحد الإجراءات الحاسمة في هذا الصدد، حيث أطلقته سنغافورة وقامت بإنشاء صندوق بقيمة 190 مليون دولار سنغافوري، أي ما يعادل 117 مليون يورو من أجل إجراء البحوث حول الأمن السيبراني خلال الفترة من 2015 إلى 2020، وهو ما يدل على تزايد الاهتمام بالفضاء السيبراني ومخرجاته الأمنية، مما سيسمح لسنغافورة بتطوير منتجات جاهزة وآمنة، يتم فيه التركيز على أنترنت الأشياء.¹⁸ كما يمكن الاستدلال كذلك على اهتمام دول الآسيان بالأمن السيبراني من خلال عدد الأبحاث التي تم إجراؤها حول الموضوع، وفي هذا الصدد نسوق هذه البيانات في الشكل التالي:

الشكل 01: عدد أبحاث الأمن السيبراني المنشورة من قبل دول الآسيان في الفترة من 2014-2019



المصدر:

Nor Shazwina Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nur hizam SafieMohdSatar, Siti Mariam Shahar, "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries", **International Journal of Advanced Trends in Computer Science and Engineering**. volume 8, No.1.4, 2019. p117. At: <https://n9.cl/hxpvf> : 10/03/2021.

يتضح من خلال معطيات هذا الشكل بأن الأمن السيبراني لا يحتل نفس الأهمية بالنسبة لدول جنوب شرق آسيا؛ إذ لم تظهر أية أبحاث في كل من لاوس وكمبوديا ولعل ذلك يعود بالدرجة الأولى إلى درجة النمو والتطور التي يعرفها كل بلد، ففي الوقت الذي تنتهياً فيه كل من ماليزيا وسنغافورة وإندونيسيا لتجسيد الاقتصاد الرقمي، تهتم كل من لاوس وكمبوديا بقضايا أخرى.

ثانياً: المبادرات الإقليمية

يعتبر الأمن السيبراني أحد أكثر المواضيع مناقشة وبحثاً بين دول رابطة أمم جنوب شرق آسيا؛ حيث عقد المؤتمر الوزاري الثاني الآسيان حول الأمن السيبراني في سنغافورة في 18 سبتمبر 2017، تم التطرق فيه إلى أهمية تطوير المعلومات، والتأكيد على البنى التحتية، كما تمت الموافقة على أهمية تعزيز التنسيق لضمان جهود الأمن السيبراني للآسيان لمواجهة التهديدات السيبرانية متزايدة التعقيد. أما القمة الخاصة بين الآسيان وأستراليا في مارس 2018 فقد تم فيها الاتفاق من أجل تعزيز التعاون لمواجهة التهديدات الإلكترونية خاصة منها الإرهاب الإلكتروني، وفي هذا الصدد تم إبرام العديد من الشراكات مع دول أخرى لتعزيز قدراتها على ضمان الأمن السيبراني نذكر منها:

1- إعلان الرابطة لمنع ومكافحة الجريمة الإلكترونية

من أجل التصدي لتزايد مشاكل الأمن السيبراني، وفي هذا الصدد طورت الآسيان برنامج آسيان للقدرة السيبرانية في أبريل 2017، ومدته خمس سنوات، من أجل المساعدة في تمويل الجهود المبذولة لتعميق القدرات السيبرانية عبر الدول الأعضاء، وبناء قدراتهم السيبرانية من خلال:

- أ. تعزيز القدرة الإقليمية على الاستجابة للتهديدات الإلكترونية.
- ب. بناء فضاء إلكتروني آمن لرابطة أمم جنوب شرق آسيا
- ج. تطوير التقنية والسياسات وبناء الاستراتيجيات
- د. تطوير استراتيجية الاستجابة للحوادث الإلكترونية

من أجل تجسيد هذا البرنامج تم تخصيص غلاف مالي قدر بـ عشرة (10) مليون دولار سنغافوري.¹⁹

2- الخطة الرئيسية لاتصال الآسيان 2020:

تهدف الخطة لتحقيق نظام تشغيل سلس وشامل للرابطة، بالشكل الذي يعزز من القدرة التنافسية الشاملة، وتعزيز الشعور بالانتماء للمجتمع، وتشمل هذه الخطة خمس مجالات استراتيجية هي: البنية التحتية المستدامة، والابتكار الرقمي، والجانب اللوجستي، والتميز التنظيمي، وتنقل الأفراد.²⁰

3- لجنة الآسيان للعلوم والتكنولوجيا COST

تعد هذه اللجنة مسؤولة عن صياغة خطة الآسيان في مجال العلوم والتكنولوجيا والابتكار، وقد تم إطلاق رؤية الآسيان للعلوم والتكنولوجيا (2016-2025) في نوفمبر 2015، وتتكون من أربعة محاور استراتيجية هي:

- أ. تعزيز التعاون الاستراتيجي بين الأوساط الأكاديمية ومؤسسات البحث والقطاع الخاص، من أجل بيئة فعالة لتطوير القدرات ونقل التكنولوجيا وتسويقها
- ب. تعزيز تنقل العلماء والباحثين، وتعزيز مشاركة الأفراد في مجالات العلوم والتكنولوجيا والابتكار.
- ج. إنشاء نظام مبتكر وتأسيس شراكة ذكية مع الآخرين، ورعاية مشاريع الابتكار والعلوم والتكنولوجيا لدعم المشاريع الصغيرة والمتوسطة لزيادة القدرة التنافسية.
- د. رفع مستوى الوعي وتنمية ثقافة العلوم والتكنولوجيا لتطوير العلوم وتعزيز التعاون التكنولوجي.

4- مبادرة تأمين الفضاء الإلكتروني للآسيان

تسعى هذه المبادرة لتأمين الفضاء من خلال:

* التدريب والتعاون والتنسيق بين دول الآسيان وبعض شركائها الرئيسيين

* تحسين الاستجابة لحالات الطوارئ الحاسوبية في الرابطة.²¹

5- برنامج التجارة الإلكترونية

إدراكا منها لإمكانيات التجارة الإلكترونية، تبنت الآسيان برنامجا للتجارة الإلكترونية كجزء مجموعة الآسيان الاقتصادية، يهتم البرنامج بالتطوير في المجالات التالية:

أ. البنية التحتية الإلكترونية

ب. كفاءة التعليم والتكنولوجيا

ج. حماية المستهلك

د. تحديث الإطار القانوني

هـ. أمن المعاملات الإلكترونية

و. اللوجستيات، المنافسة، والتجارة الإلكترونية

6- فريق (APCERT)

يتكون الفريق من أعضاء من 22 دولة آسيوية، وقد شكل ليكون شرطة إلكترونية من أجل مكافحة الجريمة السيبرانية وتأمين الفضاء السيبراني في جميع دول الآسيان بشكل أكثر فعالية.²²

ثالثا: المبادرات العالمية

سنتطرق هنا للفواعل المتعاونة مع الآسيان سواء كانوا دولاً أو منظمات إقليمية:

1- التعاون بين الآسيان والصين

تم الإعلان عام 2003 عن برنامج عمل لتنفيذ الإعلان المشترك " الشراكة من أجل السلام والازدهار" بهدف الاستجابة للطوارئ، وتعزيز الصيانة لضمان الأمن السيبراني ومكافحة الجريمة السيبرانية.

2- التعاون بين الآسيان والاتحاد الأوروبي

تمخض التعاون بين دول الآسيان والاتحاد الأوروبي عن مجموعة من التدابير والإجراءات على المستوى الدولي وعلى مستوى الإقليمي:

أ) التعاون الدولي (بين الدول)

ب) تتمثل أهم المبادرات في هذا المستوى فيما يلي:

❖ التعاون بين الاتحاد الأوروبي وسنغافورة من خلال توقيع العديد من مذكرات التفاهم لتعزيز قدرات الأمن السيبراني.

❖ التعاون بين سنغافورة وبريطانيا من أجل بناء القدرات في مجال الأمن السيبراني

❖ التعاون بين سنغافورة وهولندا من أجل تبادلات ثنائية منتظمة لأفضل ممارسات واستراتيجيات الأمن السيبراني

❖ التعاون بين فينتام وفنلندا لتعزيز تكنولوجيا المعلومات.

❖ التعاون بين ماليزيا وبريطانيا من أجل تعزيز الاقتصاد الرقمي.²³

ت) التعاون الأفريقي (بين الآسيان والاتحاد الأوروبي)

أنتج التعاون بين الآسيان والاتحاد الأوروبي (كحدثين إقليميتين) جملة من البرامج والمبادرات نذكر أهمها كالتالي:

❖ تأسيس أكاديمية التدريب السيبراني: تم إطلاقها في فيفري 2018 في جامعة آسيا والمحيط الهادي، تهدف الأكاديمية لحماية وتعزيز الأمن الرقمي في منطقة آسيا والمحيط الهادي، وتبادل المعارف وأحسن الممارسات من أجل بناء القدرات المادية والبشرية الرقمية.

❖ التعاون في مجال البحث والابتكار H2020&FP7: يتلخص التعاون في هذا المجال في برنامجين رئيسيين هما:

- برنامج التمويل HORIZON 2020: يوفر هذا البرنامج إطارا للتعاون بين الآسيان والاتحاد الأوروبي في مواضيع الأمن السيبراني؛ بحيث يهدف للمساهمة في تجسيد التآزر الاستراتيجي في بحوث تكنولوجيا المعلومات والاتصالات، وكذا تحقيق التنمية والابتكار ونقل الخبرات بين الطرفين، وذلك من خلال جملة من المشاريع أهمها:

- مشروع Connect T2SEA: يهدف هذا المشروع لتعزيز التعاون بين الطرفين من خلال وضع الأسس الاستراتيجية للشراكات ذات التأثيرات المستدامة، وقد استمر المشروع من ديسمبر 2013 إلى ماي 2016، ممولا في إطار البرنامج الإطار السابع للمفوضية الأوروبية.²⁴

- مشروع YAKSHA: يعتبر أحدث مشاريع HORIZON2020، التي تتناول الأمن السيبراني بين الاتحاد الأوروبي والآسيان، يتم تمويله في إطار ICT-39 وهي شراكة دولية بين الدول متوسطة ومنخفضة الدخل، يهدف المشروع لتعزيز التعاون وبناء شراكات بين الاتحاد الأوروبي ورابطة أمم جنوب شرق آسيا، بداية بتعزيز جاهزية دول الآسيان للأمن السيبراني من خلال استحداث آليات لمنع الهجمات الالكترونية، وتقليل المخاطر السيبرانية. ويتم اختبار مدى فعالية YAKSHA في كل من

أوروبا وجنوب شرق آسيا مع التركيز في البداية على كل من فيتنام وماليزيا واليونان. أخيرا ستقوم YAKSHA بإنشاء شهادة التميز التكنولوجي، كاعتراف مستدام بجودة المنتج وأمانه، مما سيؤدي لزيادة الطلب على المنتجات التي تحمل علامة YAKSHA للتميز.

❖ **الإطار المقترح: connect 2 SEA** الذي يهدف إلى تبادل المعرفة ونقل القدرات الفنية، ومساعدة الدول التي لا تزال في مراحلها الأولى من البحث والتطوير، ثم تعزيز التعاون الإقليمي، وفيما بين الأقاليم.²⁵

كل هذه المبادرات وأخرى إنما تعكس وعي الآسيان بضرورة التعاون في المجال الإلكتروني باعتباره أحد أهم مصادر التهديد في العصر الرقمي الذي لا يمكن مواجهته بطريقة انفرادية من قبل الدول، غير أن معطيات الدول المتباينة وأولوياتها الأمنية قد حال دون تفعيل معظم المبادرات سالفة الذكر.

خاتمة:

يمثل الفضاء السيبراني في منطقة جنوب شرق آسيا مجالا تفاعليا نشطا ومزدحما بالنظر لما يفرضه من تحديات وتهديدات وفرص في ذات الوقت، الأمر الذي دفع بدول الآسيان فرادى وجماعة لجعله مجالا أساسيا للتعاون الأمني من أجل درء تهديداته والاستفادة من فرصه، غير أن ما تملكه دول الآسيان من إمكانيات مستحدثة في هذا المجال، ونظرا لاختلاف أولويات دول الآسيان الأمنية قد شكل حدودا مثبتة لتعاون أمني إلكتروني فعال، لذلك فقد خلصت الدراسة في نهاية هذا البحث إلى النتائج التالية:

- أصبح الأمن الإلكتروني وجها مهما من أوجه الأمن القومي والإقليمي والعالمي، ودول الآسيان كنظام أمن إقليمي تسعى لبناء جماعة أمنية ليست بمنأى عن التهديدات الإلكترونية؛ إذ تحاول التكيف تدريجيا مع الابتكارات الرقمية، ما أدى إلى زيادة تعرضها للهجمات السيبرانية، خاصة مع ما تؤكد بعض الدراسات حول نقص الوعي لدى شريحة واسعة من مستخدمي الانترنت اتجاه عدة أنواع من الهجمات الإلكترونية، وهو ما يعتبر أول تحدي أمام ضمان الأمن السيبراني

- تتميز التهديدات السيبرانية بالتعقيد والتركيب والتداخل، وتطال كافة جوانب الأمن أفقيا (الأمن العسكري، والأمن السياسي، والأمن الاقتصادي، والأمن المجتمعي)، وعموديا من خلال تعرض مختلف الوحدات والفواعل الدولية للتهديدات الإلكترونية من جهة، ومن خلال حالة التداخل والتأثير المتبادل للتهديدات الإلكترونية بعضها مع بعض من جهة أخرى.

- يخضع التعاون الدولي في مجال مواجهة تهديدات الأمن السيبراني للعديد من الاعتبارات السياسية والتقنية والقانونية، مما جعل تطوره يسير على نحو بطيء على المستوى الإمبريقي، وبما لا يتناسب

وسرعة التطور التكنولوجي، وانتشار مخاطره. فحول جنوب شرق آسيا التي تعرف معظمها ديناميكية تطويرية سريعة في المجال الإلكتروني، تعرف في الوقت نفسه زيادة كبيرة في تعرضها للهجمات الإلكترونية، الأمر الذي يدل على عدم جاهزية هذه الدول إلكترونيا لحماية فضاءها الإلكتروني. -لقد شكل تباين القدرات السيبرانية بين دول الآسيان عائقا أمام تجسيد التدابير الجماعية (الإقليمية والعالمية) على الرغم من وجود اتفاق ضمني بين مختلف الفواعل على ضرورة تنسيق الجهود لمواجهة التهديدات السيبرانية متزايدة التعقيد، كما يعتبر غياب الوعي لدى شريحة واسعة من المتضررين اتجاه أنواع مختلفة من الهجمات الإلكترونية أول ثغرة تواجه الجاهزية الإلكترونية للمنطقة، ومن ثمة العجز عن ضمان الأمن السيبراني للآسيان.

التوصيات:

إن إدارة الأمن السيبراني تبدأ ببناء القدرات السيبرانية من أجل ضمان جاهزية إلكترونية للدخول في علاقات تعاونية متكافئة وفعالة، لذلك على دول الآسيان بناء قدراتها السيبرانية الفردية (الدولانية) من أجل القضاء على التباين الشديد فيما بينها بالشكل الذي يجعل من التعاون الإقليمي وحتى العالمي سلسا وفعالاً.

قائمة المصادر والمراجع:

باللغة العربية:

أولاً: الكتب:

1- البصلي جاسم محمد، الحرب الإلكترونية أسسها وأثرها في الحروب. ط2، المؤسسة العربية للدراسات والنشر، بيروت، 1989.

2- عبد الصادق عادل، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة. مركز الدراسات السياسية والاستراتيجية، مصر: القاهرة، 2009.

ثانياً: أشغال الملتقيات والمؤتمرات:

1- البداينة ذياب موسى، "الجرائم الإلكترونية: المفهوم والأسباب"، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية 2-2014/09/4، الأردن: عمان، 2014.

2- الزنط سعد عطوة، "الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي"، مؤتمر الجرائم المستحدثة - كيفية إثباتها ومواجهتها..، المركز القومي للبحوث الاجتماعية والجنائية، 15-16 ديسمبر 2010.

باللغة الأجنبية:

A. Articles In Journals:

- 1- KhanisaKrisman, "A Secure connections: finding the forme of Asean cyber Security cooperation", **journal of Asean studies**, vol.1, N° 1, 2013. At: <https://n9.cl/lppf>
- 2- Mizan Mohamed, ShazwinaNor, Ma'arif, Dr, Yusnorizam, Muhamad, *et al.* Cnds-cybersecurity: Issues and challenges in asean countries. **International Journal of Advanced Trends in Computer Science and Engineering**, vol. 8, no 1.4, 2019. At : <https://n9.cl/hxpvf>

B. Articles in cite web:

- 1- Choucri, Nazli, Madnick, Stuart, et koepke, Priscilla. "Institutions for cyber security: International responses and data sharing initiatives". Cambridge, MA: Massachusetts Institute of Technology, 2016. At: <https://cyberpolitics.mit.edu/science-security/institutions-cybersecurity>
- 3- Interpol, "aseancyberthreat assessment 2021 key cyber threat trends outlook from the asean cybercrime operations desk". on: www.interpol.int
- 4- Sociedade Portuguesa de Inovação, "Overview of Cyber security Status in ASEAN and the EU", Version 1.1 (v.1.1), 2018. At: <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bedd4ced&appId=PPGMS>

الهوامش:

- ¹: عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة. مركز الدراسات السياسية والاستراتيجية، القاهرة، 2009، ص ص 96-99.
- ²: المرجع نفسه. ص ص 110-113.
- ³: سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي، مؤتمر الجرائم المستحدثة - كيفية إثباتها ومواجهتها..، المركز القومي للبحوث الاجتماعية والجنائية، 15-16 ديسمبر 2010، ص 2.
- ⁴: المرجع نفسه. ص ص 252-257.
- ⁵: موسى نيا ببدانية، الجرائم الإلكترونية: المفهوم والأسباب، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية 2-4/09/2014، عمان -الأردن، 2014، ص ب.
- ⁶: المرجع نفسه. ص 2.
- ⁷: عادل عبد الصادق، مرجع سابق. ص ص 133-134.
- ⁸: جاسم محمد البصيلي، الحرب الإلكترونية أسسها وأثرها في الحروب. ط2، المؤسسة العربية للدراسات والنشر، بيروت، 1989، ص ص 41-42.
- ⁹: المرجع نفسه. ص 137.
- ¹⁰: Nazli Choucri Stuart Madnick Priscilla Koepke, 'Institutions for Cyber Security: International Responses and Data Sharing Initiatives', **Working Paper CISL# 2016-10 August 2016**, pp 8- 9. At: <https://cyberpolitics.mit.edu/science-security/institutions-cybersecurity>
- ¹¹: **Interpol**, asean cyber threat assessment 2021 key cyber threat trends outlook from the asean cybercrime operations desk, 2021. p 11. At: www.interpol.int : 04/04/2021.
- ¹²: **Interpol**, **opcit.** p 11.
- ¹³: Sociedade Portuguesa de Inovação, 'Overview of Cyber security Status in ASEAN and the EU', Version 1.1 (v.1.1), 2018, p 62.at: <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bedd4ced&appId=PPGMS>: 10/03/2021.
- ¹⁴: **Ibid.** p 64.
- ¹⁵: **Idem.**
- ¹⁶: **Ibid.** p 79.
- ¹⁷: Nor Shazwina, Mohamed Mizan, Muhamad Yusnorizam Ma'arif, NurhizamSafie, MohdSatar, Siti Mariam Shahar, 'CNDS-Cyber security: Issues and Challenges in ASEAN Countries', **International Journal of Advanced Trends in Computer Science and Engineering**.volume 8, No.1.4, 2019. Pp 114- 115.At: <https://n9.cl/hxpvf> : 10/03/2021.
- ¹⁸: Sociedade Portuguesa de Inovação, **op.cit.** p 61.
- ¹⁹: **Ibid.** p 10-11.
- ²⁰: **Ibid.**p8.
- ²¹: **Ibid.** p 64.
- ²²: Krisma Khanisa, **op.cit.** P 43.
- ²³: Sociedade Portuguesa de Inovação ,**op.cit.** P 68.
- ²⁴: **Ibid.** P70.
- ²⁵: **Ibid.** p 73.