الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا

د. وفـــاء لـطـفـي *

مستخلص

يعد الإرهاب السيبراني أحد أهم القضايا التي تحتل حيزا مهما في الدراسات والنقاشات المثارة على الساحة الدولية خلال الفترة الأخيرة، وهو من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت، وتتّضح خطورة هذا الإرهاب من خلال النظر إلى حجم التهديدات التي يفرضها على الأمن القومي للدول.

تعد الحرب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، ومن الناحية النظرية، فهي تغني الأنشطة الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية.

وعليه، تحاول هذه الدراسة تتبع تأثير ظاهرة الارهاب السيبراني على الدولة الماليزية والجهود المبذولة في مجال مكافحتها، حيث اصبح من أهمية بمكان أن نبحث في السبل التي يجب اتباعها للتصدي لتلك الجرائم العابرة للحدود والتي تستلزم تحديد ماهيتهاوخصائصها وطبيعتها وخصائص مرتكبيها وكيفية مساءلتهم.

كلمات مفتاحية: الإرهاب السيبراني، الحرب السيبرانية، القوة السيبرانية، الجريمة السيبرانية، ماليزيا.

Abstract:

Cyber terrorism is one of the most important issues that occupies an important space in the studies and discussions raised in the international arena during the recent period, and it is one

* مدرس العلوم السياسية، كلية الاقتصاد والادارة، جامعة ٦ أكتوبر.

- Email: wafaalotfydr@yahoo.com

of the most dangerous types of crimes committed via the Internet, and the danger of this terrorism becomes clear by looking at the size of the threats it poses to the national security of countries.

Cyber war is one of the most prominent features of political and commercial conflicts between countries, and in theory, it means malicious activities through the Internet supported by a state, targeting infrastructure or government facilities and institutions, industrial networks and research, and is able to disrupt the operation of critical infrastructure with Reducing the risk of conflict or geopolitical war.

Accordingly, this study attempts to track the impact of the phenomenon of cyber terrorism on the Malaysian state and the efforts made in the field of combating it, as it has become of great importance to discuss the ways that must be followed to address these cross-border crimes, which require defining their nature, characteristics, nature, characteristics of the perpetrators and how to hold them accountable.

Key Words: Cyber terrorism, cyber warfare, cyber power, cyber crime, malaysia.

قائمة الاختصارات

المصطلح	الاختصار
International Multilateral Partnership Against Cyber Terrorism	**IMPACT**
Center for Strategic and International Studies	**CSIS**
Certificate Authority	**CA**
Malaysian Communications and Multimedia Commission	**MCMC**
Court of Arbitration for Sport	**Cas**
Internet service providers	**ISP**
The Digital Signature Act	**DSA**
National Cyber Security Policy	**NCSP**
Critical National Information Infrastructure	**CNII**
Malaysia Defence Technology Park	**MDSTP**
International Telecommunication Union	**ITU**

مقدمة:

تختلف الجرائم السيبرانية كثيراً عن الجرائم التقليدية من حيث طبيعتها ونطاقها ووسائلها وأدلتها. فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية أما بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي والوطني، فلابد من إيجاد سبل للتصدي لهذه الظاهرة.

تتسم الجرائم السيبرانية بطابع سرية الهوية والا تترك سوى القليل من الاثر، بالاضافة إلى ذلك لا تقف امام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا.[1]

تجدر الاشارة أن قضية أمن المعلومات قد تجاوزت مفهومها التقني لتشمل الأبعاد الأمنية والدفاعية والاستراتيجية، فضلا عن أنها أصبحت جزءًا لا يتجزأ من خطط الأمن القومي والمواثيق الدفاعية للتحالفات العسكرية.

كما انها باتت محل اهتمام دائم في ظل التطور التكنولوجي المذهل الذي بقدر ما يحمله للعالم من فرص فإن في طياته مخاطر جمة، ومن ثم حاجة دول العالم الماسة إلى تشريعات دولية واضحة ومحددة بشأن مواجهة الإرهاب السيبراني.[2]

ويهدف برنامج أمن الفضاء الإلكتروني والتقنيات الحديثة على وجه الخصوص إلى تعزيز قدرات الدول الأعضاء على منع الهجمات الإلكترونية التي تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية. كما يسعى البرنامج أيضاً إلى تخفيف تأثير هذه الهجمات الإلكترونية واستعادة وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات.[3]

تعد الحرب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، من الناحية النظرية يقصد بالحرب السيبرانية الأنشطة الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية.

وسواء كان الهجوم السيبراني مرتبطاً مباشرة بوكالة حكومية أم لا، فقد تكون له عواقب مدمرة، لا سيما إذا استهدف بنية تحتية حيوية.[٤]

فقد أصبحت الجرائم السيبرانية أكثر تعقداً، نظراً للتطور التكنولوجي مثل أنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وخدمات من قبيل برنامج حماية الخصوصية أونيون روتر والشبكة الخفية. كل هذه التكنولوجيا تعتبر سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات ولكن تجلبها أيضا لمرتكبي جرائم معينة.

فقد أصبحت القضايا المتعلقة بالارهاب السيبراني مصدر قلق خطير لانها تشكل خطراً على الامن القومي الماليزي.

وعلية تواجه الحكومات المزيد من التحديات في مجال مكافحة استخدام تكنولوجيا المعلومات والاتصالات للاغراض الاجرامية.

ان السبب الرئيسي في انتشار الارهاب السيبراني هو أن الإرهابي لا يحتاج إلى أداة متفجرة أو عالية التقنية للقيام بمهاجمة الضحية ولكنه يحتاج فقط إلى نقل الفيروسات أو البرامجيات الخبيثة أو سرقة المعلومات باستخدام اجهزة التكنولوجيا الحديثة. كل هذا يساعد الارهابي ان يكون غير معلوم الهوية مما يقلل من خطر وقوعه في أيدي السلطات.

من هذا المنطلق تَطرح هذه الدراسة تساؤلًا رئيسيًّا هو: ما الاستراتيجيات والسياسات التي تتبناها الدولة الماليزية في مجال مكافحة ظاهرة الإرهاب السيبراني؟

ومن هذا التساؤل الرئيسي تثار مجموعة من التساؤلات الفرعية وهي كالتالي:

- ما المقصود بالإرهاب السيبراني وما الذي يميزه عن غيره من المفاهيم المشابهة؟
- ما هي خصائص الارهاب السيبراني؟ وما هي أبرز مخاطره؟
- ما هي أهم الاستراتيجيات التي اتبعتها الدولة الماليزية في مكافحة جرائم الارهاب السيبراني؟
- ما هي مبادرات الحكومة الماليزية في مكافحة الجرائم الإلكترونية؟
- وما الجهود الماليزية في مكافحة الجرائم السيبرانية؟

أهمية الدراسة

تحاول الدراسة القاء الضوء على ظاهرة الإرهاب السيبراني التي أصبحت من أخطر القضايا الدولية في العصر الحاضر نظراً لاتساع نطاق استخدام

التكنولوجيا الحديثة في العالم، لذا من الاهمية بمكان معرفة أسبابه لمعرفة كيفية مكافحته في ظل قلة الدراسات والبحوث حولها.

كما تنبع أهمية الدراسة من كونها تعتبر دراسة استكشافية تسعى إلى رصد جريمة الإرهاب السيبراني في ماليزيا، والجهود التي تبذلها الدولة لمكافحتها، وهي تقييمية تسعى إلى تقييم جهود الدوله في مجال مكافحة جريمة الإرهاب السيبراني.

أهداف الدراسة

تسعى الدراسة إلى تحقيق عدة أهداف، أهمها:

- إبراز خطورة ظاهرة الإرهاب السيبراني على الأمن القومي الماليزي.
- محاولة الوقوف على العوامل المؤدية لانتشار ظاهرة الارهاب السيبراني في المجتمع الماليزي.
- القاء الضوء على استراتيجيات وآليات الدولة الماليزية في التعامل مع ظاهرة الارهاب السيبراني ومكافحتها والحد من انتشارها.

تقسيم الدراسة

تُقسَّم الدراسة إلى ثلاثة محاور على النحو الآتي:

المحور الأول: ماهية جريمة الإرهاب السيبراني، ويتناول تعريف الإرهاب السيبراني، والتمييز بينه وبين المفاهيم المتداخله معه، ثم بيان خصائص الارهاب السيبراني ومخاطره وصوره.

المحور الثاني: الجهود الماليزية في مكافحة جريمة الإرهاب السيبراني، ويشتمل الجهود المتبعة من قبل الدولة الماليزية لمكافحة الإرهاب السيبراني.

المحور الثالث: يتناول تحديات الأمن السيبراني في ماليزيا والتهديدات الدولية المتزايدة عبر الإنترنت.

المحور الرابع:

أهم استراتيجيات ماليزيا في مجال مكافحة جريمة الإرهاب السيبراني تشريعيا وتنفيذيا.

مقدمة:

تختلف الجرائم السيبرانية كثيراً عن الجرائم التقليدية من حيث طبيعتها ونطاقها ووسائلها وأدلتها. فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية أما بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي والوطني، فلابد من إيجاد سبل للتصدي لهذه الظاهرة.

تتسم الجرائم السيبرانية بطابع سرية الهوية والا تترك سوى القليل من الاثر، بالاضافة إلى ذلك لا تقف امام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا.[٥]

تجدر الاشارة أن قضية أمن المعلومات قد تجاوزت مفهومها التقني لتشمل الأبعاد الأمنية والدفاعية والاستراتيجية، فضلا عن أنها أصبحت جزءًا لا يتجزأ من خطط الأمن القومي والمواثيق الدفاعية للتحالفات العسكرية.

كما انها باتت محل اهتمام دائم في ظل التطور التكنولوجي المذهل الذي بقدر ما يحمله للعالم من فرص فإن في طياته مخاطر جمة، ومن ثم حاجة دول العالم الماسة إلى تشريعات دولية واضحة ومحددة بشأن مواجهة الإرهاب السيبراني.[٦]

ويهدف برنامج أمن الفضاء الإلكتروني والتقنيات الحديثة على وجه الخصوص إلى تعزيز قدرات الدول الأعضاء على منع الهجمات الإلكترونية التي تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية. كما يسعى البرنامج أيضاً إلى تخفيف تأثير هذه الهجمات الإلكترونية واستعادة وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات.[٧]

تعد الحرب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، من الناحية النظرية يقصد بالحرب السيبرانية الأنشطة الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية.

وسواء كان الهجوم السيبراني مرتبطاً مباشرة بوكالة حكومية أم لا، فقد تكون له عواقب مدمرة، لا سيما إذا استهدف بنية تحتية حيوية.[٨]

فقد أصبحت الجرائم السيبرانية أكثر تعقداً، نظراً للتطور التكنولوجي مثل أنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وخدمات من قبيل برنامج حماية الخصوصية أونيون روتر والشبكة الخفية. كل هذه التكنولوجيا تعتبر سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات ولكن تجلبها أيضا لمرتكبي جرائم معينة.

فقد أصبحت القضايا المتعلقة بالارهاب السيبراني مصدر قلق خطير لانها تشكل خطراً على الامن القومي الماليزي.

وعلية تواجه الحكومات المزيد من التحديات في مجال مكافحة استخدام تكنولوجيا المعلومات والاتصالات للاغراض الاجرامية.

ان السبب الرئيسي في انتشار الارهاب السيبراني هو أن الإرهابي لا يحتاج إلى أداة متفجرة أو عالية التقنية للقيام بمهاجمة الضحية ولكنه يحتاج فقط إلى نقل الفيروسات أو البرامجيات الخبيثة أو سرقة المعلومات باستخدام اجهزة التكنولوجيا الحديثة. كل هذا يساعد الارهابي ان يكون غير معلوم الهوية مما يقلل من خطر وقوعه في أيدي السلطات.

من هذا المنطلق تَطرح هذه الدراسة تساؤلًا رئيسيًّا هو: ما الاستراتيجيات والسياسات التي تتبناها الدولة الماليزية في مجال مكافحة ظاهرة الإرهاب السيبراني؟

ومن هذا التساؤل الرئيسي تثار مجموعة من التساؤلات الفرعية وهي كالتالي:

- ما المقصود بالإرهاب السيبراني وما الذي يميزه عن غيره من المفاهيم المشابهة؟
- ما هي خصائص الارهاب السيبراني؟ وما هي أبرز مخاطره؟
- ما هي أهم الاستراتيجيات التي اتبعتها الدولة الماليزية في مكافحة جرائم الارهاب السيبراني؟
- ما هي مبادرات الحكومة الماليزية في مكافحة الجرائم الإلكترونية؟
- وما الجهود الماليزية في مكافحة الجرائم السيبرانية؟

أهمية الدراسة

تحاول الدراسة القاء الضوء على ظاهرة الإرهاب السيبراني التي أصبحت من أخطر القضايا الدولية في العصر الحاضر نظراً لاتساع نطاق استخدام

التكنولوجيا الحديثة في العالم، لـذا مـن الاهميـة بمكـان معرفـة أسـبابه لمعرفـة كيفية مكافحته في ظل قلة الدراسات والبحوث حولها.

كما تنبع أهمية الدراسة من كونهـا تعتبـر دراسـة استكشـافية تسـعى إلـى رصـد جريمة الإرهاب السيبراني في ماليزيـا، والجهـود التـي تبـذلها الدولـة لمكافحتهـا، وهي تقييمية تسعى إلى تقييم جهود الدولـه فـي مجـال مكافحـة جريمـة الإرهـاب السيبراني.

أهداف الدراسة

تسعى الدراسة إلى تحقيق عدة أهداف، أهمها:

- إبراز خطورة ظاهرة الإرهاب السيبراني على الأمن القومي الماليزي.
- محاولـة الوقـوف علـى العوامـل المؤديـة لانتشـار ظـاهرة الارهـاب السيبراني في المجتمع الماليزي.
- القاء الضوء على استراتيجيات وآليات الدولة الماليزيـة فـي التعامـل مـع ظاهرة الارهاب السيبراني ومكافحتها والحد من انتشارها.

تقسيم الدراسة

تُقسَّم الدراسة إلى ثلاثة محاور على النحو الآتي:

المحـور الأول: ماهيـة جريمـة الإرهـاب السـيبراني، ويتنـاول تعريـف الإرهـاب السيبراني، والتمييز بينـه وبـين المفـاهيم المتداخلـه معـه، ثـم بيـان خصـائص الارهاب السيبراني ومخاطره وصوره.

المحـور الثـاني: الجهـود الماليزيـة فـي مكافحـة جريمـة الإرهـاب السـيبراني، ويشتمل الجهود المتبعة من قبل الدولة الماليزية لمكافحة الإرهاب السيبراني.

المحور الثالث: يتناول تحديات الأمن السـيبراني فـي ماليزيـا والتهديـدات الدوليـة المتزايدة عبر الإنترنت.

المحور الرابع:

أهم استراتيجيات ماليزيا في مجـال مكافحـة جريمـة الإرهـاب السـيبراني تشـريعيا وتنفيذيا.

المحور الأول: ماهية جريمة الإرهاب السيبراني

اولا: الارهاب السيبراني.

عرفت الموسوعة السياسية الإرهـاب بأنـه :"اسـتخدام العنـف غيـر القـانوني، أو التهديد به بأشكاله المختلفـة كالاغتيـال والتشـويه والتعـذيب والتخريـب والنسـف، بغية تحقيق هدف سياسي معين مثل كسـر روح المقاومـة والالتـزام عنـد الأفـراد، وهدم المعنويات عند الهيئات والمؤسسات، أو كوسيلة مـن وسـائل الحصـول علـى

المعلومات أو مال، وبشكل عام هو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية".[٩]

في ثمانينيات القرن العشرين كان أول ظهور لمفهوم الإرهاب السيبراني Cyberterrorism ، فقد عرفه باري كولين Barry Collin بأنه "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيًا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب".[١٠]

وفي عام ١٩٩٨، نشر المشروع العالمي للجريمة المنظمة التابع لمركز الدراسات الإستراتيجية والدَّولية في واشنطن CSIS تقريرًا بعنوان "جرائم الإنترنت والإرهاب الإلكتروني والحرب الإلكترونية: تجنب حدوث ووترلو إلكترونية" ' Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo'، والذي كان يعتبر أولَ مساهمة رئيسة في هذا المجال.[١١]

وتعرف دورثي دينينغ Dorothy Denningg الإرهاب السيبراني على انه "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمرًا وتخريبيًّا لتوليد الخوف بحيث يكون مشابهًا للأفعال المادية للإرهاب".[١٢]

يعرفه "جيمس لويس" James Lewiss على أنه "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل، والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين.[١٣]

وتعرفه وزارة الدفاع الامريكي بأنه "عمل إجرامي يتم الاعداد له باستخدام الحاسبات ووسائل الاتصالات وينتج عنه عنف وتدمير أو بث الخوف تجاه متلقى الخدمات بما يسبب الارتباك وعدم اليقين".[١٤]

ويعرفه مكتب التحقيقات الفيدرالي الارهاب السيبراني على انه "الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر، والبيانات المخزنة من قبل مختلف الفاعلين".

ويعرف الإرهاب السيبراني على انه نقطة التقاء الفضاء الإلكتروني والإرهاب، وهو يشير إلى الهجمات والتهديدات غير القانونية بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها عندما يتم ذلك لتخويف أو إكراه حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية.[١٥]

وهو التهديد أو الهجوم غير القانوني بشن هجماتٍ على أجهزة الكمبيوتر، وأنظمة المعلومات، والبرامج، والبيانات، بهدف ترهيب وإكراه الحكومات تحقيقًا لمختلف الأهداف.

والارهاب السيبراني هو محاولة خبيثة ومتعمدة من قبل فرد أو منظمة لاختراق نظام المعلومات الخاص بفرد أو مؤسسة .[١٦]

يميز البعض من الباحثين بين نوعين من الإرهاب السيبراني، يشير أولهما إلى الإرهاب السيبراني الخالص Pure Cyber Terrorism، والذي يتصل بالهجمات المباشرة على البنيه التحتية للضحية لتحقيق أهداف مختلفة. بينما يُشير الثاني إلى الإرهاب السيبراني الهجينHybrid Cyber Terrorism، وفيه يستخدم الارهابيون الفضاء السيبراني في مختلف الانشطة كالدعاية والحرب النفسية، والتخطيط لهجمات أرهابية فعلية، وتجنيد أعضاء جدد، وجمع الاموال، والتبرعات... الخ[١٧]

<u>هناك تداخل بين مفهوم الارهاب السيبراني وبين عدد من المفاهيم الاخرى سنتعرض لها بايجاز وهي:</u>

<u>القوة السيبرانية</u>

يعرفها دانيال كوين على أنها " استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في جميع البيئات العملياتية وعبر أدوات القوة.

ويقصد بالعملياتية المجالات الخمسة للقوة وهي البحرية، والبرية، والجوية، والفضائية والفضاء السيبراني.

كما يقصد بأدوات القوة، الابعاد الأربعة للقوة والمتمثلة في الدبلوماسية ، والمعلومات، والاقتصاد، والجيش.[١٨]

<u>الجريمة السيبرانية</u>

لا يوجد تعريف محدد للجريمة السيبرانية، فهناك من يعرفها على انها " كل فعل ضار بالآخرين عبر استعمال الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الانترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموما.[١٩]

ويعرفها آخرون بأنها " نشاط إجرامي نشاط إجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.[٢٠]

الحرب السيبرانية.

يقصد بالحرب السيبرانية اساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح.

اي هي الهجمات والعمليات التي ترتكب ضد او بواسطة شبكات الحواسيب وانظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، او سياسات الردع المتبادل.[٢١]

وتعد الحروب السيبرانية ميدان رابع من ميادين الحروب فهي حروب خفية تقتحم الأنظمة الإلكترونية وتسبق العمل العسكري.

تستهدف الحرب السيبرانية استهداف الأنظمة العسكرية والبنية التحتية الحيوية للدولة فضلا عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها.[٢٢]

تصنف الهجمات السيبرانية ضمن أبرز المخاطر التي تحيط بالدول، حيث زادت حجم الهجمات السيبيرانية بين الدول في الفترة الحالية . لذلك قامت الدول بتخصيص وحدات إلكترونية خاصة بالأمن السيبراني وزادت من حجم صلاحياتها. [٢٣]

الأمن السيبراني.

الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. وعادة ما تهدف هذه الهجمات الإلكترونية إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، ابتزاز المال من المستخدمين، أو مقاطعة العمليات التجارية العادية.[٢٤]

البيئة الرقمية

تعرف البيئة الرقمية على انها سياق او مكان يتم تمكينه بواسطة التكنولوجيا والأجهزة الرقمية، التي غالباً ما تنتقل عبر الإنترنت، أو غيرها من الوسائل الرقمية، مثل شبكة الهاتف المحمول. تشكل السجلات والأدلة على تفاعل الفرد مع البيئة الرقمية بصمتها الرقمية.[٢٥]

ثانيا: خصائص الارهاب السيبراني

للارهاب السيبراني العديد من الخصائص التي تميِّزه عن الإرهاب في صورته التقليدية، والتي تسعى في نهاية الأمر لتحقيق أهداف غير مشروعة، وهي:[٢٦]

١. أن الإرهاب السيبراني إرهاب عابر للقارات والحدود، وغير خاضعة لنطاق اقليمي محدود.

٢. صعوبة اكتشاف أثر الجاني في مرتكب واقعة الإرهاب السيبراني، حيث يوجد العديد من الصعوبات التي تقف حائلًا دون الوصول لدليل مادي يربط الجاني بالواقعة.

٣. الارهاب السيبراني يعد أحد أخطر أنواع الإرهاب، إذ انه يؤثر بالسلب على الأمن القومي للدولة المستهدفة. وفي هذا الصدد يقول بيتر غرابوسكي أن طريقة توظيف تقنية المعلومات الواسعة تعتبر وسيلة لتسهيل الإرهاب، ومن ذلك قرصنة المعلومات الاستخباراتية، واستخراج البيانات، وجمع الأموال، والتوظيف والتعبئة والتدريب عن بعد، مثل التدريب على استخدام تقنية الهجوم ومهاراته، ومشاركة المعلومات، ونشر الأدلة، مثل أدلة صنع الأسلحة وغيرها.[٢٧]

٤. الارهاب السيبراني لا يحتاج عند ارتكابه الى العنف والقوة بل يتطلب حاسب الي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، لذا يوصف بأنه من قبيل الجرائم الناعمة التي لا تتطلب استخداما للقوة في معناها العنيف أو المسلح.

٥. مرتكب الجريمة السيبرانية لديه الخبرة في استخدام تكنولوجيا المعلومات، وبالتالي تكون أهدافه ليست صعبة، وبالتالي صعوبة الاثبات قيامه بالجريمة، نظرا لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره.

ثالثا: مخاطر الارهاب السيبراني.

في عام ٢٠١٩ أكَد تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي، أن الإرهاب السيبراني أصبح واقعا لا مفر منه.

ويصف التقرير الهجَماتِ السيبرانيةَ بأنها تلك الهجَماتُ التي تتسبَّب في أضرار اقتصادية كبيرة، أو اضطرابات جيوسياسية، أو مشاهدَ ومواقف تتصدع فيها الثقة بشبكة الإنترنت على نطاق شاسع.

وتتمثل الهجَمات الإرهابية واسعة النطاق بأفراد أو جماعات غير الحكومية ذات أهداف سياسية أو دينية أو اجتماعية تهدف إلى إلحاق أضرار بشرية أو مادية واسعة النطاق.

وفي هذا الاطار كشف تقرير المنتدى الاقتصادي العالمي عن مخاطرَ عميقة للهجوم الإرهابي السيبراني، حيث أنه له صلة وثيقة بانهيار البِنية التحتية للمعلومات الهامة، وخطر إطلاق أسلحة الدمار الشامل. وقد تتعدد طرائق العمل من استعمال البرامج التخريبية الخبيثة و(فيروسات) البرامج، إلى حجب الخِدْمات، والأعمال الاستخباراتية التجسُّسية على الشبكة وغيرها.[٢٨]

رابعا: الاتفاقيات الدولية في مكافحة الجرائم السيبرانية.

معاهدة بودابست لمكافحة جرائم الانترنت

تعد هذه الإتفاقية هى أولى الإتفاقيات العالمية المتعلقة بجرائم الانترنت، وقعت الإتفاقية في العاصمة المجرية بودابست في ٢٣ نوفمبر ٢٠٠١، بهدف التعاون والتضامن الدولى فى محاربة الجرائم الإلكترونية.

وقعت ٢٦ دولة أوروبية على هذه الإتفاقية بالإضافة إلى الولايات المتحدة الامريكية، كندا واليابان، جنوب أفريقيا.[٢٩]

وبالرغم من ان هذه الاتفاقية أوروبية المنشأ، إلا ان عضويتها مفتوحة لجميع الدول التي تريد الانضمام إليها لتعم الفائدة.

وعلى الرغم من أن هذه الإتفاقية لا تعالج الإرهابَ السيبرانى على وجه الخصوص، إلا أنها صيغت بطريقة قادرة على تتبع نطاق تهديدات الإرهابيين، لتشمل جريمة الإرهاب السيبراني.

فى عام ٢٠١٦ أصدرت لجنةُ اتفاقية الجرائم السيبرانية مذكرةً توجيهية تتعلَّق بجوانب الإرهاب السيبرانى بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الإتفاقية قد تكون أيضًا أعمالا إرهابية على النحو المحدد في القانون المعمول به". وجاءت هذه المذكرة الإضافية بموجب الإتفاقية فى الوقت المناسب، لتسلط المذكرة الضوء على أن هذه الإتفاقية ليست معاهدة مختصة بالإرهاب، إلا أنه يمكن القول: إن الجرائم الموضوعية فى الإتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانبُ التمويلي، أو الأعمال التحضيرية.[٣٠]

المحور الثاني:الجهود الماليزية في مجال مكافحة جريمة الارهاب السيبراني

تتعدد الجهود التي تبذلها الدول في مجتمع المعلومات العالمي من اجل العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع الارهاب السيبراني من قبل الحكومات.

قد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الاقليمي وذلك من أجل حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الاخطار.[٣١]

ففي ظل التحولات الرقمية التي يعيشها العالم بوجه عام وماليزيا بوجه خاص ظهر نوع جديد من التهديدات الأمنية التى تعتبر البيئة الرقمية عاملا هاما في

انتشارها، وقد أصبحت هذه التهديدات تمس ليس فقط أمن المؤسسات وإنما أمن الأفراد وبذلك تكون شكلت تحديا للدوله في سعييها لتحقيق أمنها القومي.

وقد استمرت الدولة الماليزية في تطوير سياسات وبرامج تساعدها في تعزيز أمنها السيبراني في إطار رؤية ٢٠٢٠.[٣٢]

ويجدر بالذكر أن الهدف من إطلاق رؤية ماليزيا ٢٠٢٠ هو أن تصبح دولة متقدمة واعتناق الاقتصاد القائم على المعرفة كوسيلة لتحقيق ذلك.

ومن خلال الاختيار الواعي لاستخدام تكنولوجيا المعلومات والاتصالات كأداة للتنمية، فقد أدى ذلك إلى زيادة استخدام أنظمة المعلومات الرقمية في جميع أنحاء الصناعة والمنظمات الخاصة والعامة والمجتمع ككل.

ومما شك فيه إن الاعتماد على أنظمة المعلومات الرقمية يجلب معه نقاط الضعف والمخاطر المتزايدة، لا سيما للبنية التحتية للمعلومات الوطنية الحرجة (CNII) والتي تشمل من بين أمور أخرى الجرائم الإلكترونية مثل القرصنة والتطفل والاحتيال والمضايقة والرموز الضارة وهجمات الحرمان من الخدمة، كل ذلك يزيد التهديدات السيبرانية التي تهدد السيادة الإلكترونية للدولة.[٣٣]

تم إنشاء العديد من مواقع الانترنت لمكافحة الإرهاب السيبراني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية او من القطاع الخاص او من المجتمع المدني ، فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

تعد ماليزيا إحدى الدول التي كثفت جهودها في هذا المجال منذ وقت مبكر، كونها دخلت المجتمع المعلوماتي في وقت متزامن مع العديد من دول العالم المتقدم، فقد تم تصنيفها من قبل الخبراء والمتخصصين في مرتبة متقدمة نظرا للانجازات التي حققتها حتى الآن للإندماج في مجتمع المعلومات.[٣٤]

منذ عام ١٩٨٧ دخلت خدمة الانترنت إلى ماليزيا من قبل المعهد الماليزي للأنظمة الإلكترونية الدقيقة، وذلك من خلال مشروع رنجكوم Rangkom، الذي قام بربط عدة جامعات ماليزية في شبكة واحدة.

في عام ١٩٩١ تحول مشروع رنجكوم Rangkom إلى مزود خدمة يعرض خدماته لعدد محدود من العامة.

وفي عام ١٩٩٢ تم إطلاق أول مزود ماليزي لخدمات الانترنت RARING، أطلقه المعهد الماليزي للانظمة الإلكترونية الدقيقة.[٣٥]

حيث تفوقت ماليزيا على دول الاسيان بما في ذلك تايلاند التي جاءت في المرتبة الـ ١٣ وفيتنام التي جاءت في المرتبة الـ ١٤ والفلبين التي جاءت في المرتبة الـ ١٨ واندونسيا جاءت في المرتبة الـ ٢٠.[٣٦]

وقد ازداد ظهور أنشطة الإرهاب السيبراني بوضوح في ماليزيا في العِقد الماضي، ورفعت دعاوى قضائية بموجب قانون العقوبات في البلاد وتصنف الأحكام تحت الرقم (ج-٠٣١) والرقم (ي-٠٣١) مختلِف الأعمال المرتكبة في سياق الأعمال الإرهابية.

سعت الدولة الماليزية الى تكثيف جهودها الرامية إلى مكافحة الجرائم الإلكترونية أو استخدام الإنترنت لأغراض إرهابية، بما في ذلك تعزيز المرافق الأمنية للإنترنت وتشديد الرقابة على أنظمة التواصل الإلكتروني.[٣٧]

تضع ماليزيا الأمن السيبراني نصب أعينها وتحاول أن تكون نموذجاً لمنطقة آسيا والمحيط الهادي، حيث أنها تقدم ما يقرب من اثنتي عشرة خدمة تلبي احتياجات القطاع العام والقطاع الخاص ومستخدمي الانترنت.

تشريعات وقوانين مكافحة الارهاب السيبراني في ماليزيا

تعد ماليزيا واحدة من اولى الدول في جنوب شرق آسيا التي سنت قوانين وتشريعات الفضاء السيبراني، فهناك عدة قوانين وتنظيمات تبنتها الدولة الماليزية للتعامل مع الارهاب السيبراني والتي كان من أهمها:[٣٨]

١. **قانون جرائم الكمبيوتر عام ١٩٩٧:**[٣٩]

هو أول تشريع محدد على الإطلاق يتم في ماليزيا لمكافحة الجرائم الإلكترونية. يجرم عمل القراصنة ونشر الفيروسات على اجهزة الكمبيوتر والاتصال غير المشروع للوصول إلى أجهزة الكمبيوتر وارتكاب الجرائم الإلكترونية.

٢. **قانون التوقيع الرقمي عام ١٩٩٧.**

التوقيع الرقمي هو توقيع إلكتروني يستخدم للتحقق من هوية المرسل / الموقّع للرسالة وأيضًا لضمان صحة المعلومات في المعاملات الإلكترونية، ويمكن أن يفي استخدام التوقيع الرقمي المعترف به بمتطلبات السرية ، ومصادقة الهوية، وعدم التنصل، وسلامة المعلومات.

دخل قانون التوقيع الرقمي لعام (DSA) حيز التنفيذ في ١ أكتوبر ١٩٩٨، بهدف تنظيم استخدام التوقيع الرقمي في ماليزيا، ويضمن أمن القضايا القانونية المتعلقة بالمعاملات الإلكترونية ويتحقق من استخدام التوقيعات الرقمية من خلال الشهادات الصادره عن المرجع المصدق المرخص (CA).[٤٠]

تعتبر هيئة الاتصالات والوسائط المتعددة الماليزية (MCMC) مسؤولة عن إدارة وتنفيذ أحكام DSA 1997 لغرض المراقبة والإشراف على أنشطة CAs.

٣. **قانون الاتصالات والوسائط المتعددة عام ١٩٩٨:**[٤١]

تم سنّ القانون في عام١ نوفمبر ١٩٩٨ – كان بمثابة تشريع في عام ١٩٩٧– وقد أجريت تعديلات المره الاولى في عام ٢٠٠٢ والمره الثانية في ١ يناير ٢٠٠٦.

ونص على إنشاء لجنة الاتصالات والوسائط المتعددة الماليزية مع صلاحيات الإشراف على الاتصالات والأنشطة المتعددة الوسائط في وتنظيمها، وتطبيق قوانين الاتصالات والوسائط المتعددة.

٤. **قانون حماية البيانات الشخصية عام ٢٠١٠:**[٤٢]

يهدف قانون حماية البيانات الشخصية الصادر في عام ٢٠١٠ إلى ضمان عدم إساءة أستخدام أي بيانات شخصية يتم جمعها كما يفرض على الشركات الحصول على موافقة من الأفراد قبل جمع بياناتهم الشخصية أو مشاركة بياناتهم مع أطراف أخرى، فضلا القانون وضع شروط تسجيل لمستخدمي البيانات في صناعات معينة وإلا فإن ذلك قد يعرضهم لعقوبة جنائية بحد أقصى ٥٠٠٠٠٠ رينغيت ماليزي أو ما يصل إلى ثلاث سنوات في السجن، أو كليهما.

المحور الثالث:تحديات الأمن السيبراني في ماليزيا والتهديدات الدولية المتزايدة عبر الإنترنت

وفقاً لدراسة أجراها الاتحاد الدولي للاتصالات (ITU) تعد ماليزيا واحدة من أكبر عشر دول مستهدفة بهجمات البرامج الضارة على مستوى العالم.

شهدت ماليزيا خرقًا هائلاً للبيانات التي نشأت بسبب البرامج الخبيثة، وكان التأثير المالي ضخمًا بسبب اختراق البيانات. كما أن الوعي بالأمن السيبراني في ماليزيا لم يتم توصيله بشكل جيد لجميع المواطنين.

وفقاً لاحصائية قدمها فريق الاستجابة لحالات طوارئ الكمبيوتر، والذي يعمل في إطار Cyber Security Malaysia أن هناك من ٢,٧ مليون من هجمات الربوتات الآلية وهجمات عدوى البرامج الضارة بواسطة بروتوكولات الانترنت الفريدة (IPS)

كما كشفت إحصائيه أخرى أنه تم الإبلاغ عن أكثر من ٩٠٠٠ قضية تتعلق بالأمن السيبراني في ماليزيا، مثل المضايقات الإلكترونية والاحتيال والتطفل والرموز الخبيثة ورفض الخدمة والمحتوى المرتبط بالبريد العشوائي.

تزايدت حوادث الجرائم الإلكترونية بمعدل ينذر بالخطر في ماليزيا ومنطقة جنوب شرق آسيا حيث شهدت المنظمات المزيد من الهجمات الإلكترونية، حيث يستغل مجرمو الإنترنت في ماليزيا الخوف وعدم اليقين المحيطين بتفشي فيروس كورونا.

تم اكتشاف ٢٠ برنامجًا ضارًا مختلفًا مرتبطًا بفيروس كورونا من قبل متخصصي الأمن السيبرانيKaspersky، وذكرت مجلة Forbesأن ماليزيا هي واحدة من أكثر خمس دول في العالم مستهدفة من قبل مجرمي الإنترنت أثناء تفشي المرض واصبح معدل الهجمات الإلكترونية في تزايد عن زي قبل.[٤٣]

وكشفت شركة Microsoft في دراسة أجريت عام ٢٠١٨ أن ماليزيا قد عانت من خسائر اقتصادية بلغت ١٢,٢ مليار دولار أمريكي بسبب الجرائم السيبرانية[٤٤]

واكتشفت شركة Technisanct الناشئة للأمن السيبراني أن أكثر من ٣٥٠٠٠ بطاقة ائتمان من عدد من البنوك قد تم اختراقها في ماليزيا وتم بيعها على شبكة الإنترنت.

وقد اطلقت أحدى الشركات التكنولوجية حلاً أطلق Linkdood منصة اتصالات صممها خبراء الأمن السيبراني لتمكين الموظفين من تخزين الملفات والتعاون بأمان باستخدام تقنية السحابة الخاصة.

أطلقت LGMS، وهي شركة محلية للأمن السيبراني ، مختبرًا للأمن السيبراني مع مزود الخدمة النمساوي TÜV Austria

قال سفير النمسا في ماليزيا الدكتور مايكل بوستل: "هذه الشراكة لديها القدرة على ترسيخ ماليزيا كمركز لاختبار واعتماد الأمن السيبراني لمنطقة آسيا والمحيط الهادئ."

وقد حققت شركة البيانات الماليزية Strateq أيضًا نجاحًا مؤخرًا عندما أعلنت شركة الاتصالات السنغافورية StarHub أنها ستدفع ما يصل إلى ٨٢ مليون دولار سنغافوري مقابل حصة تبلغ ٨٨٪ في الشركة.

وتعمل ماليزيا على إنشاء نظام دفاع إلكتروني متطور اكتمل الآن بنسبة ٩٠٪ بعد ثلاث سنوات من العمل، وإذا سار العمل وفقًا للخطة ، فستكون ماليزيا في طريقها لتصبح واحدة من أفضل القدرات في المنطقة.

وقد وقعت منظمة Cyber Security Malaysia_المرتبطة بالحكومة أيضًا اتفاقية مع Blackberry لحماية بعض البيانات الأكثر أهمية وحساسية في ماليزيا من مجرمي الإنترنت.

تظهر ماليزيا بوادر تحسن في الحرب ضد مجرمي الإنترنت وجدت دراسة حديثة أجرتها شركة Cisco أن الشركات في ماليزيا تلقت تنبيهات إلكترونية أقل بنسبة ٣٪ في عام ٢٠١٩ مقارنة بعام ٢٠١٨ ، وهو أفضل من المتوسط في منطقة آسيا والمحيط الهادئ. وذكرت الدراسة أيضًا أن الاتهاكات التي تكلف الشركات مليون دولار أمريكي أو أكثر انخفضت من ٥٠٪ في ٢٠١٨ إلى ٢٣٪ فقط في ٢٠١٩ .

لكن المعركة لم تنته بعد. ما زال أمام ماليزيا ومنطقة آسيا والمحيط الهادئ طريق طويل لتقطعه، ولا تزال المنطقة تتلقى المزيد من التنبيهات على أساس يومي أكثر من المناطق الأخرى التي شملتها الدراسة التي أجرتها شركة Cisco.

بينما شهد عدد التنبيهات التي تم التحقيق فيها أيضًا انخفاضًا في جميع أنحاء المنطقة منذ عام ٢٠١٨.

وضعت الدولة للمستهلكين والعملاء ومستخدمي الإنترنت عدد من الطرق التي يمكن من خلالها المساعدة في منع الجرائم الإلكترونية منها: لابد من استخدام كلمة مرور مختلفة لكل حساب، تجنب الوصول إلى المعلومات الحساسة وحفظ التفاصيل الخاصة بك عند استخدام شبكة WiFi العامة، قراءة رسائل البريد الإلكتروني بعناية لتجنب هجمات التصيد الاحتيالي، لابد من مراجعة عناوين مواقع الويب والتحقق مما إذا كانت آمنة. [٤٥]

المحور الرابع: أهم الاستراتيجيات والسياسات التي تَبَنَّتْها الدوله لمكافحة الإرهاب السيبراني

تعد ماليزيا أكثر دول جنوب شرق اسيا تقدما في استراتيجية الأمن السيبراني وإن ريادة ماليزيا في هذا المجال تنبثق من تأسيس وكالة وطنية لتعزيز وتنسيق جدول أعمال الأمن السيبراني وصياغة القوانين والخطة الشاملة لتنمية المهنيين في المجال نفسه.

الهجمات السيبرانية العابرة للحدود تفتح مجالا لهذه البلاد للتعاون مع خبراء الأمن السيبراني وصانعي السياسة ورواد الأعمال وصناع القرار التجاري في هذه المنطقة من أجل تعزيز مرونة الآسيان.

منذ التسعينات والدولة الماليزية تحاول تكييف سياساتها لتستجيب للتهديدات الجديدة المرافقة للبيئة الرقمية، ووسعت دائرة التعاون مع القطاع الخاص، فضلاً عن أنها وضعت عددا مهما من التنظيمات القانونية لتعزيز أمنها السيبراني.

ولحماية الحكومة والشركات من أي الهجمات السيبرانية تنفذ وزارة الدفاع الماليزية السياسة الأمنية لتكنولوجيا المعلومات، من بين مهامها ضمان سلامة الشبكات ومنع الحوادث الإلكترونية من إحداث آثار اقتصادية ضارة.

في عام ٢٠٠٦ أعلنت ماليزيا إطلاق مبادرة تحت مسمى " الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الالكتروني IMPACT، وقد تضمن تلك المبادرة انشاء أربعة مراكز وهي: مركز تنمية المهارات والتدريب، مركز لشهادات الامن والبحث والتنمية، مركز دعم التعاون الدولي، مركز الاستجابة والطوارئ الدولية.

لمكافحة الارهاب السيبراني تم إنشاء العديد من مواقع الانترنت بمبادرة من الحكومة او القطاع الخاص أو مؤسسات المجتمع المدني فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات، وأصبحت بمثابة مؤسسات فكرية لدعم الأمن الرقمي.[٤٦]

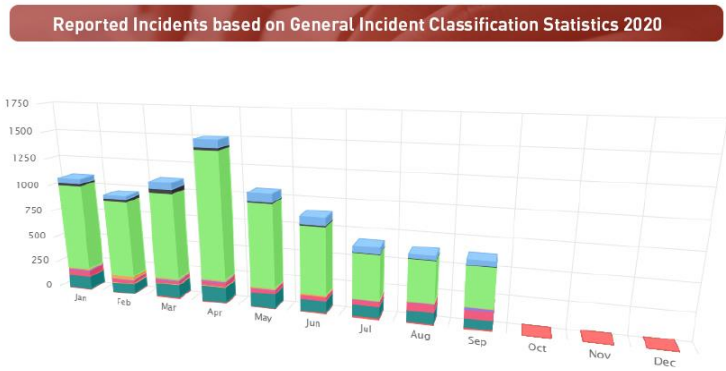
وضعت وزارة الاتصالات والوسائط المتعددة استراتيجية ٢٠١٩- ٢٠٢٣ تركز على تعزيز أمن الفضاء الإلكتروني في البلاد وزيادة الوعي العام بالاستخدام الحكيم والأخلاقي للأجهزة الرقمية.

وفي ٢٠٢٠ اطلقت ماليزيا مشروع تجريبي لأمن الانترنت والنهوض بالمهارات في مجال الأمن الالكتروني والصناعة، ويعزز من كفاءة ممارسي الأمن الإلكتروني الحاليين، ويساهم في رعاية جيل جديد من المتخصصين الموثوق بهم في مجال الأمن الإلكتروني وبالتالي يعزز القدرة التنافسية في الدفاع عن الفضاء الإلكتروني الوطني".[٤٧]

وفي سعي الدولة لتعزيز التأهب الوطني للأمن السيبراني تم تكليف وزارة الاتصالات والوسائط المتعددة والوكالة الوطنية للأمن السيبراني بمهمة صياغة خطة العمل متوسطة الأجل، فضلًا عن تنفيذها وتنسيقها. [٤٨]

شكل رقم (١) [٤٩]

شكل يوضح تطور الجرائم السيبرانية في ماليزيا في الفترة من يناير إلى سبتمبر ٢٠٢٠



مبادرات الحكومة الماليزية في مكافحة الجرائم السيبرانية:

تحت إشراف وزارة الوسائط المتعددة والاتصالات (MCMC) ، تم تأسيس CyberSecurity Malaysia باعتبارها وكالة متخصصة في الأمن السيبراني لتقديم مجموعة واسعة من الخدمات وتعزيز اعتماد ماليزيا على ذاتها في الفضاء الإلكتروني.

وتقوم المنظمة بمساعدة وكالات إنفاذ الطب الشرعي والتحليل السيبراني، مثل تحليل الأدلة وتوفير خبراء لقضايا الجرائم الإلكترونية، فضلا عن ترسيخ ثقافة الأمن من خلال برامج التوعية. [٥٠]

إلى جانب CyberSecurity Malaysia ، هناك أيضًا العديد من المنظمات الفرعية والخدمات المقدمة لتلبية حاجة ماليزيا المتزايدة للأمن عبر الإنترنت. [٥١]

وبالرغم من أن المعلومات حول الارهابيين السيبرانيين تعتبر في الغالب معلومات سرية ولا يمكن الكشف عنها بسهولة إلا أنه يمكننا أستنتاج وجود هذا النوع من التهديد في ماليزيا وذلك من خلال بعض الاحداث التي وقعت وأربكت الحكومة الماليزية.

وقد جاءت تلك الهجمات بعد تحذير جماعة أطلقت على نفسها " المجهول Anonymous، والتي قالت أنها ستهاجم البوابات الرئيسية للحكومة لمعاقبتها على فرض رقابة على موقع ويكيليكس الذي يقوم بتسريب الوثائق السرية للشركات متعددة الجنسيات والحكومات.[٥٢]

ومن أهم الانشطة السيبرانية كانت نشاطات حركة "التنظيف Persih"، والتي تبنت أستخدام وسائل الإعلام الرقمية منذ أن تأسست في ٢٣ نوفمبر ٢٠٠٦ ، وخلال السنوات التالية شهدت عملياتها في الوسائط الرقمية تطورا كبيرا.

فقد جعلت هذه الحركة من استخدام المواقع والمدونات واليوتيوب أدوات رئيسية للتداول والتعبئة مع استخدامات متقطعة لـ Flickr.

وقد كان التدوين خياراً طبيعاً أضافة إلى إدماج يوتيوب وفليكر في عام ٢٠٠٦، والفيسبوك في ٢٠٠٨، وتويتر في ٢٠١١، الذي لم يكن مفاجئا في ظل شعبية هذه المنصات بين الماليزيين وخاصة الشباب.[٥٣]

في عام ٢٠١١ نظمت حركة Pershi[٥٤]، حمله احتجاجية من أجل الإصلاح الديمقراطي في ماليزيا وأستخدمت فيها بشكل واسع الهواتف الذكية وشبكات التواصل الاجتماعي.

هناك العديد من السياسات والبرامج التي وضعتها الحكومة الماليزية للتصدي للإرهاب السيبراني نذكر منها ما يلي:

١. **السياسة الوطنية للأمن السيبراني (NCSP):**

اتخذت الحكومة مبادرات للتخفيف من الهجمات الإلكترونية ومكافحتها. إحدى المبادرات التي تم اتخاذها هي تطوير السياسة الوطنية للأمن السيبراني (NCSP)، والتي أقرتها الحكومة في مايو ٢٠٠٦. [٥٥]

وهي عباره عن تطبيق مالي شامل للأمن السيبراني يتم تنفيذه بطريقة متكاملة لضمان حماية البنيه التحتية الوطنية Critical National Information Infrastructure (CNII) إلى مستوى يتناسب مع المخاطر التي تواجهها، عبر الأجهزة الحكومية، واجتذب التنفيذ العديد من الوزارات والوكالات للعمل معًا لتلبية رؤية وجود CNII مضمون ومرن ومعتمد على الذات من شأنه في النهاية تعزيز الاستقرار والرفاهية الاجتماعية وخلق الثروة للبلد.

يتكون برنامج NCSP من ثمانية (٨) توجهات سياسية وهي:[٥٦]

- الحوكمة الفعالة.
- الإطار التشريعي والتنظيمي.
- إطار تكنولوجيا الأمن السيبراني.

- ثقافة الأمن وبناء القدرات.
- البحث والتطوير نحو الاعتماد على الذات.
- الامتثال والتنفيذ.
- الجاهزية للطوارئ الأمنية السيبرانية والتعاون الدولي.

وبعد ٤ سنوات من تنفيذ برنامج NCSP ، يُنظر الآن إلى الأمن السيبراني في ماليزيا على أنه شيء لا يستهان به، حيث تم إنجاز الكثير ولا يزال يتعين القيام بالمزيد مع تغير مشهد التهديدات السيبرانية مع تطور التقنيات والأدوات الجديدة.[٥٧]

٢.البنية التحتية الوطنية الحرجة للمعلومات.

تُعرِّف البنية التحتية للمعلومات الوطنية الحاسمة (CNII) بأنها تلك الأصول (الحقيقية والافتراضية) والأنظمة والوظائف الحيوية للدول التي سيكون لعجزها أو تدميرها تأثير على القوة الاقتصادية الوطنية، الدفاع والأمن القومي، وقدرة الحكومة على العمل بكفاءة، الصحة العامة والسلامة.[٥٨]

- **برنامج الأمن السيبراني الماليزي:**

تم تصميم Malaysia CyberSecurity ، وهو برنامج تابع لوزارة العلوم والتكنولوجيا والابتكار الماليزية، لتكون قادرة على التخفيف من التهديدات السيبرانية.

لهذا السبب، تسعى CyberSecurity Malaysia إلى إقامة شراكات وتعزيز جهود التعاون مع الدول والمنظمات الدولية.

تحاول ماليزيا إنشاء منصات متعددة الأطراف للأمن السيبراني مثل مركز آسيا والمحيط الهادئ (APCERT) ومنظمة التعاون الإسلامي (OIC-CERT)، من أجل التخفيف من التهديدات السيبرانية الدولية.

برنامج التوعية المعروف باسم CyberSAFE – Cyber Security Awareness For Everyone ، هو مبادرة CyberSecurity Malaysia لتثقيف وتعزيز وعي الجمهور بالمسائل التكنولوجية والاجتماعية التي تواجه مستخدمي الإنترنت، ولا سيما بشأن مخاطر الاتصال بالإنترنت. CyberSAFE في المدارس. فضلا عن أن البرنامج يهدف إلى الوصول إلى جيل الشباب في المدارس لآنها تضم الجزء الأكبر من مستخدمي الإنترنت.[٥٩]

٣.الحضيرة الماليزية لتكنولوجيا الدفاع MDSTP Malaysia Defence Technology Park

تعتبر الحضيرة الاولى من نوعها في منطقة الاسيان –وفق تصريح لوزير الدفاع الماليزي Zahid Hamide– لتلبية الطلب واحتياجات الصناعة الدفاعية وألامنية المتزايدة، وتهدف إلى تحقيق مجموعة من الاهداف لعل أهمها يتمثل في:[٦٠]

- دفع ماليزيا إلى اقتصاد قائم على الابتكار، وذلك من خلال استضافة المركز الأكثر تقدمًا وتكاملاً للبحث والتطوير، وإنتاج منتجات مبتكرة ذات صلة بصناعة الدفاع.
- تسهيل أنشطة البحث والتطوير الدفاعي والابتكار والتسويق من خلال توفير البنية التحتية والمعدات والمرافق المتطورة.
- تعزيز تطوير بيئة مواتية لتقنيات ومنتجات الدفاع الفكرية والإبداعية والمبتكرة.
- تسهيل الشراكات الذكية بين الحكومة والقطاع الخاص في تطوير تكنولوجيا الدفاع وتسويق نتائج البحوث.
- إعداد مزودي صناعة الدفاع المحليين للمشاركة في مناقصة العقود العالمية.
- تمكين مزود الصناعات الدفاعية المحلي والدولي من تصنيع منتجات للسوق المحلي والإقليمي والعالمي.

٤. **فريق الاستجابة لطوارئ الكمبيوتر الماليزي MYCERT**

يعد فريق الاستجابة للطوارئ الحاسوبية في ماليزيا ('MyCERT') ذراع الاستجابة للأمن السيبراني في ماليزيا، لتوفير نقطة اتصال لمستخدمي الإنترنت المتأثرين بالحوادث المتعلقة بالأمن.

- **مركز المساعدة Cyber999**

تتوفر خبرة الاستجابة للطوارئ مساعدة الجمهور الماليزي على اكتشاف وتفسير والاستجابة لحوادث أمن الكمبيوتر مثل المضايقات الإلكترونية والبرامج الضارة والهجمات المستهدفة.

- **CyberCSI**

خدمات الطب الشرعي الرقمي ذات النطاق الكامل، والتدريب والشهادات ، بالإضافة إلى استعادة البيانات، وتعقيم البيانات، وخدمات التقاضي للحكومة ووكالات إنفاذ القانون والمنظمات الخاصة.

- **Cyber DEF**

الكشف عن التهديدات والقضاء على التهديدات وتحليل الأدلة الجنائية المخصص لتأمين البنى التحتية الوطنية للأمن السيبراني.[٦١]

وفي عام ٢٠١٥ أنشأت القوات المسلحة الماليزية وحدة دفاع الكتروني لحماية المعلومات السرية المتعلقة بنظام الدفاع من التسريب أو الاختراق. وتراقب هذه الوحدة عن كسب الأنشطة الإلكترونية التي تشكل تهديداً محتملاً لنظام الدفاع في البلاد.

كما أنها تعمل أيضا من أجل تعزيز نظام الدفاع السيبراني وإجراء عمليات تدقيق الموقف الأمني بالأضافه إلى الطب الشرعي الالكتروني.

تخضع وحدة الدفاع السيبراني لسلطة شعبة استخبارات أركان الدفاع *، وهي وكالة المخابرات العسكرية التابعة للقوات المسلحة.

تهدف الوكالة إلى عولمة الأمن السيبراني، وتوسيع المبادرات من خلال التعاون الثنائي والمتعدد الأطراف مع الوكالات المحلية والدولية وذلك لتعزيز استراتيجيات الأمن السيبراني للدولة.[٦٢]

على الرغم من الجهود التى تبذلها الدولة الماليزية في مكافحة الارهاب السيبراني إلا أن هناك العديد من التحديات التي تواجه الدوله في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية لعل من أهمها:[٦٣]

١. نقص الموارد البشرية لدى وكالات إنفاذ القانون يشكل تحدِّياً تواجهه السلطات الوطنية، اذ ان بعض وكالات إنفاذ القانون في ماليزيا لا يوجد لديها فريق مكرس للتركيز على التحقيقات في الجرائم السيبرانية.
٢. حاجة الدولة إلى رفع مستوى مهارات وكفاءات القضاة والمدعين العامين وتعزيز معارفهم بشأن أساسيات تكنولوجيات المعلومات والاتصالات والأمن السيبراني، بما في ذلك معرفة المصطلحات المتعلقة بالنظم الحاسوبية والشبكات.
٣. على أجهزة إنفاذ القانون الحصول على الأدلة الرقمية عبر الحدود من خلال قناة رسمية، وهي المساعدة القانونية المتبادلة، لكي تكون الأدلة مقبولة في المحكمة. وقد يستغرق تلقي الردود من خلال هذه المساعدة وقتاً طويلاً للغاية، مما قد يطيل إجراءات المحكمة. وبالإضافة إلى ذلك، لا تزال طلبات الحصول على الأدلة خارج الولاية القضائية تخضع لمسألة ازدواجية التجريم.
٤. أن الشركات الماليزية الصغيرة والمتوسطة من المحتمل أن يكون ٣٣% منها عرضة للهجمات الإلكترونية ويرجع السبب في ذلك إلى عدم وعيهم بأمن المعلومات مما يؤدي إلى إدارة عشوائية لمعلوماتهم وأصولهم الرقمية.
٥. ماليزيا بحاجة إلى تطوير نظام بيئي وطني للابتكار في مجال الأمن السيبراني للاستجابة للتهديدات السيبرانية المتزايدة التعقيد.

الخاتمة

حاولت الدراسة أن تجيب على التساؤلات التي تم طرحها في بداية الدراسة، وتمثلت الإجابات في النقاط الآتية:

١. الإرهاب السيبراني أصبح خطراً عالمياً يتطلب استجابة دولية وتعاونا أمميا، وأصبحت الحاجة ملحه إلى سياسة مشتركة وإطار تشريعي مشترك.
٢. نستنتج من العرض السابق أن أمن المعلومات التحدي الأكبر الذي يتطلب صياغة الخطط والاستراتيجيات للتعامل مع مخاطره، وفي الوقت ذاته تدريب المزيد من الكوادر البشرية التي يكون بمقدورها ليس فقط مواجهة تلك المخاطر بل إجهاض محاولات اختراق الأجهزة والمؤسسات المختلفة وخاصة الأمنية والدفاعية منها، وهذا هو التحدي الحقيقي الذي تواجهه كل دول العالم بوجه عام وماليزيا بوجه خاص.
٣. تم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الالكتروني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية أو من القطاع الخاص أو من المجتمع المدني، فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

التوصيات

وتقدم الدراسة عددًا من التوصيات التي تعتمد بالأساس على:

١. ضرورة التعاون وتضافر الجهود في جمع المعلومات الاستخبارتية وتبادلها.
٢. التعاون والتآزر الدولي في التحقيقات والملاحقات القضائية.
٣. التعاون بين االوكالات والشراكة بين القطاعين العام والخاص.
٤. ابتكار طرق وكيفيات تعزز من القوة السيبرانية لتحقيق مصالح الامن القومي والمصالح القومية.
٥. النهوض بالذكاء الاصطناعي.

هوامش الدراسة

[١] تقرير الامم المتحدة، **مكافحة استخدام تكنولوجيا المعلومات والاتصالات للاغراض الاجرامية**،ص ٤٨.

[٢] د.شريف محمد كشك، **آلية جديدة للأمن السيبراني في الدول دول الخليج**، على الرابط التالي:
http://www.akhbar-alkhaleej.com/news/article/1217656

[٣] **أمن الفضاء الالكتروني**، الامم المتجدة، مكتب مكافحة الارهاب، على الرابط التالي:
https://www.un.org/counterterrorism/ar/cybersecurity

[٤] ما هي خلفية استراتيجية الصين في الحرب السيبرانية؟، على الرابط التالي:
https://www.mc-doualiya.com/chronicles

[٥] تقرير الامم المتحدة، **مكافحة استخدام تكنولوجيا المعلومات والاتصالات للاغراض الاجرامية**،ص ٤٨.

[٦] د.شريف محمد كشك، **آلية جديدة للأمن السيبراني في الدول دول الخليج**، على الرابط التالي:
http://www.akhbar-alkhaleej.com/news/article/1217656

[٧] **أمن الفضاء الالكتروني**، الامم المتجدة، مكتب مكافحة الارهاب، على الرابط التالي:
https://www.un.org/counterterrorism/ar/cybersecurity

[٨] ما هي خلفية استراتيجية الصين في الحرب السيبرانية؟، على الرابط التالي:
https://www.mc-doualiya.com/chronicles

[٩] عبد الوهاب الكيالي، **الموسوعة السياسية**، ج٧ (بيروت : المؤسسة العربية للدراسات والنشر، ١٩٩٤)، ص١٥٣.

[١٠] عادل عبد الصادق، **الإرهاب الإليكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة** (القاهرة: مركز الدراسات السياسية والاستراتيجية،٢٠٠٩)، ص١٠٩.

[١١] عبد الستار عبد الرحمن، **الارهاب السيبراني خطر يهدد العالم**، على الرابط التالي:
https://imctc.org/Arabic/ArticleDetail/Index/637180424114481635

[12] Denning,Dorothye.,"**Cyber terrorism**",Global Dialogue,Aug 2000, p10
https://smtcenter.net/?p=8215

[١٣]

[١٤] صليحة محمدي، الارهاب الالكتروني والامن القومي للدول: نمط جديد وتهديدات مختلفة، **المجلة الجزائرية للامن والتنمية**، ص ٦٧.

[15] R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," *Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 2, pp. 149–158, 2012.

[16] What Are the Most Common Cyber Attacks?:
https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[١٧] رغدة البهي، **الارهاب السيبراني: المفهوم والسمات والانماط**، المركز المصري للفكر والدراسات الاستراتيجية، على الرابط التالي:
https://www.ecsstudies.com/7141

[١٨] د. فريدة طاجين، **سياسات الدفاع المالية في ظل التهديدات الأمنية للبيئة الرقمية: الوقع والتحديات**، ص٣٤٢.

[١٩] http://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

[٢٠] محمود أحمد القرعان، **الجرائم الإلكترونية** (عمان: دار وائل للنشر والتوزيع، الطبعة الاولى، ٢٠١٧)، ص١١.

[٢١] هالة أحمد الرشيدي، هل من حرب سيبرانية بين الولايات المتحدة وروسيا؟، جريدة الاهرام، ٤ يناير ٢٠٢١.

[٢٢] حمدون إ. تورية، **البحث عن السلام السيبراني** ، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، ٢٠١١، ص ص ٨، ٩.

[٢٣] https://www.europarabct.com

24 _____,What Is Cybersecurity?:
https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[25] ----, What is Digital Environment,
https://www.igi-global.com/dictionary/models-of-competences-for-the-real-and-digital-world/7610

[٢٦] علي عدنان الفيل، **الإجرام الإلكتروني: دراسة مقارنة**، ط١(بيروت: منشورات زين القانونية، ٢٠١١)، ص٧٤.
[٢٧] بيتر غرابوسكي، **جرائم الحاسب الالي..الابعاد العالمية في: القيادة العامة لشرطة أبو ظبي.. شبكات الانترنت وتأثيراتها الاجتماعية والامنية**، مركز البحوث والدراسات الامنية، القيادة العامة لشرطة أبوظبي،٢٠٠٦ ، ط١ ، ص٣٣٨.
[٢٨] د. سُني ذو الهدى، **تهديد الأرهاب السيبراني– وإمكانية تطبيق اتفاقية الجرائم السيبرانية**، على الرابط التالي:
https://imctc.org/arabic/ArticleDetail/Index/637285074665439022
[٢٩] منير محمد الجهيني، ممدوح محمد الجهيني، **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها** (الإسكندرية: دار الفكر العربي، ط ٢٠٠٤)، ص٩٦.
[٣٠] المرجع السابق.
[٣١] عادل عبد الصادق، **الفضاء الالكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق**(القاهرة: الهيئة العامة للكتاب، ٢٠١٨)، ص ٤٨٥.
[32] Lee Kam Hing and Tan Chee-Beng (editors), **The Chinese in Malaysia** (New York: oxford university Press,2000). p150.
[33] Mohd Shamir b Hashim, Malaysia's National Cyber Security Policy: The country's cyber defence initiatives:
https://ieeexplore.ieee.org/document/5978782
[٣٤] د. فريدة طاجين، **مرجع سابق**، ص ٣٣٩.
[35] _____، ISP List In Malaysia
http://isp-in-malaysia.blogspot.com/2011/04/isp-listing.html
[36] Neville, Spykerman**, Malaysia second in world broadband penetration ranking**, Monday, 28 Oct 2013
https://www.thestar.com.my/news/nation/2013/10/28/broadband-penetration-muhyiddin-yassin
[٣٧] _____، **ماليزيا تكثف جهودها لمكافحة الجرائم الإلكترونية**، على الرابط التالي:
https://aswaqpress.com/electronic-attacked-in-malaysia
[38] Chew Kherk Ying, **Cybersecurity 2020**:
https://practiceguides.chambers.com/practice-guides/cybersecurity-2020/malaysia
[٣٩] https://chialee.com.my/knowledge-hub/basics-of-cyber-security-law-in-malaysia.
[٤٠] https://www.mcmc.gov.my/en/sectors/digital-signature.
[٤١] https://wipolex.wipo.int/ar/legislation/details/9913
[٤٢] https://www.mcmc.gov.my/en/sectors/digital-signature.
انظر ايضا:
رمزي رشدي الدبك، **إخراج قانون حماية البيانات الشخصية من "القمقم" أصبح ضرورة مُلِّحّة**، على الرابط التالي:
http://factjo.com/Articles.aspx?Id=2433
[٤٣] W.Media, **Malaysia wages war on cybercrime**, Published 10 April 2020: https://w.media/malaysia-wages-war-on-cybercrime/
[44] I bid.
[45] I bid.
[٤٦] عادل عبد الصادق، مرجع سابق، ص ٤٨٨.
[٤٧] **ماليزيا تكثف جهودها لمكافحة الجرائم الإلكترونية**، مرجع سابق.
[٤٨] _____، **ماليزيا تطلق استراتيجيات الأمن السيبراني ٢٠٢٠-٢٠٢٤**، وكالة الأنباء الوطنية الماليزية – برناما//ب.ع س.هـ، على الرابط التالي:
https://www.bernama.com/ar/news.php?id=1889180
[49] Siti Farhana Sheikh Yahya, The rise of cybercrime in Malaysia - what you need to avoid, Oktober 25, 2020 03:27 MYT

https://www.astroawani.com/berita-malaysia/the-rise-of-cybercrime-in-malaysia-what-you-need-to-avoid-264890

[٥٠] المرجع السابق.

[51] Liau Y-Sing, Niluksi Koswanage, Hackers disrupt 51 Malaysian government websites, https://www.reuters.com/article/us-malaysia-hackers-idUSTRE75F06Y20110616

[٥٢] المرجع السابق.

[٥٣] د. فريدة طاجين، مرجع سايق، ص ٣٤٨.

[٥٤] البرسيه **Pershi** هو تحالف مكون من ٦٢ منظمة غير حكومية تسعى إلى إصلاح النظام الانتخابي الوطني تم تشكيله رسميا في ٢٣ تشرين الثاني (نوفمبر) ٢٠٠٦. ويمكن تلخيص دعوة بيرسيه في ثماني نقاط:

١. تنظيف السجل الانتخابي وخلوه من المخالفات.
٢. إصلاح نظام الاقتراع البريدي لضمان تمكين جميع المواطنين من ممارسة حقهم في التصويت.
٣. استخدام الحبر الذي لا يمحى الوصول الحر والعادل إلى وسائل الإعلام.
٤. ٢١ يومًا كحد أدنى لفترة الحملة.
٥. تعزيز وإصلاح المؤسسات العامة للعمل بشكل مستقل.
٦. دعم القوانين.
٧. وحماية حقوق الإنسان.
٨. وقف الفساد.

تم طرح النقاط الأربعة الأولى في عام ٢٠٠٧ ، وأضيف الباقي في عام ٢٠١١.

انظر: Lim M. Sweeping the Unclean: **Social Media and the *Bersih* Electoral Reform Movement in Malaysia**. Global Media Journal. 2016, 14:27. https://www.globalmediajournal.com/open-access/sweeping-the-unclean-social-media-and-the-bersih-electoral-reformmovement-in-malaysia.php?aid=83245

[55] Z. Yunos, R. Ahmad, S. M. Ali, and S. Shamsuddin, "Illicit Activities and Terrorism in Cyberspace : An Exploratory Study in the Southeast Asian Region," in Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2012), Malaysia, 29 May, Springer Lecture Notes in Computer Science, Volume 7299/2012, 2012, pp. 27–35.

[56] Z. Yunos, "Illicit Activities and Terrorism in Cyberspace," in Proceeding of CENS-GFF CyberSecurity Forum – The Geostrategic Implications of Cyberspace, 2011, pp. 12–13.

[٥٧] Mohd Shamir b Hashim, I bid.

[٥٨] https://cnii.cybersecurity.my/main/about.html

[59] Zahri Bin Yunos, **Addressing Cyber Terrorism Thr**eats, Homeland security and Defense, 7-01-2017: https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybersecurity-malaisia/

[60] Malaysia Defence Security Technology Park project, signed RM700 Million deal with USA: https://forum.lowyat.net/topic/1813457/all

[٦١] CyberSecurity Malaysia, In pursuit of Its charter, CyberSecurity Malaysia has left no stone unturned: https://www.fireeye.com/customers/cybersecurity-malaysia-customer-story.html

[*] تمتلك البحرية الملكية الماليزية غواصتين من طراز Scorpene ضمن أسطولها KD Tunku Abdul Rahman و KD Tun Abdul Razak.

[٦٢] https://knepublishing.com/index.php/KnE-Social/article/view/5052/10147

[٦٣] تقرير الامم المتحدة، مرجع سابق، ص ٥٥.