سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية : الواقع والتحديات

Malaysia's Defense Policies under the Security Threats of the Digital Environment: Reality and Challenges

د/فريدة طاجين

استاذة محاضرة في العلاقات الدولية

قسم العلوم السياسية بجامعة قاصدي مرباح ورقلة

ملخص:

رغم أنه لا يمكن التشكيك في أن الإنتشار الواسع لاستخدام تكنولوجيا المعلومات والاتصالات سهل نشاطات الانسان اليومية، إلا أن تزايد الاعتماد على تلك الوسائل يعني تزايد احتمالات التعرض للهجوم من خلالها، وفي ظل استمرار تنامي التهديدات الأمنية الناتجة عن البيئة الرقمية، سعت عدة دول إلى توسيع نطاق أمنها القومي لتضيف إليه البعد السيبراني، وتدافعت نحو إنشاء وتنفيذ استراتيجيات وسياسات دفاعية تتماشى مع التحولات السريعة في أنماط التهديدات الأمنية الناشئة. فوفقا لدراسة اجريت سنة 2015 احتلت ماليزيا المرتبة الأولى بين الأمم الأكثر ذكاءا في المجال السيبراني في اقليم آسيا والمحيط الهادي، غير أن هذا الذكاء لم ينعكس ايجابيا على أمنها السيبراني، حيث حققت في نفس الوقت لقب الدولة الأكثر قلقا على أمنها السيبراني، وهذه المعضلة تعني أن مسألة الأمن وتحقيقه في العصر الرقمي أضحت أكثر صعوبة وتعقيدا من السابق. وفي هذا السياق تسعى هذه الورقة البحثية إلى تشخيص واقع السياسات الدفاعية الماليزية وتحديد ومناقشة تحدياتها في ظل توسع وتنوع تلك التهديدات. وقد تم من أجل ذلك توظيف نظرية الأمننة لمدرسة كوبنهاغن كإطار نظري، فيما تم اتباع الاسلوب الكيفي كمنهج للبحث من خلال جمع وتحليل المعلومات الواردة في وثائق وتقارير رسمية صدرت عن شخصيات ومؤسسات حكومية ماليزية ودولية، بالإضافة إلى تقارير لمؤسسات بحثية ومقالات منشورة لباحثين في هذا المجال، وتحاول هذه الورقة المساهمة بفتح النقاش مع الباحثين المهتمين بتوسيع وتعميق فهم العلاقة بين المتغير الأمني والبيئة الرقمية الراهنة والتي لاتزال في حاجة إلى تكثيف البحوث حولها.

الكلمات المفتاحية: سياسات الدفاع، البيئة الرقمية، القوة السيبرانية، التهديدات السيبرانية، الأمن السيبراني، ماليزيا.

Abstract:

Despite it cannot be questioned that the widespread use of information and communication technologies made the everyday human activities easier, the growing use of these technologies means the increased chances of being attacked through it. In the light of the continued growth of the security threats posed by the digital environment, several countries sought to expand the scope of its national security to add the cyberspace dimension, moreover, it competed to create and precede a defensive strategies and policies in line with the rapid shift in the emerging security threat patterns. According to a study conducted in 2015, Malaysia was ranked first among the most cyber-savvy nations in the Asia-Pacific region, but this cyber savviness did not reflect on the lifting of its cybersecurity, on same time Malaysia was the country that worried the most about its cybersecurity, which means that the issue of security in the digital age has become more

difficult and complex than ever. In this context, This research paper aims to address the reality of the Malaysian Defense Policy, and identify and discuss its challenges under the various security threats of the digital environment, to this end, the securitisation theory of Copenhagen school has been applied as a theoretical framework, and a qualitative research method using a different type of Documents has been used to collect data and information. This paper attempts to contribute by opening a scientific discussion among the researchers whom interested in deepening and broadening the understanding of the correlations between the security variable and the current digital environment that still needs more studies to conduct about.

Key words: Defense Policies, Digital Environment, Cyber power, Cyber Threats, Cyber Security, Malaysia.

مقدمة

بعد التزايد السريع لحجم ووتيرة اندماج الأفراد والقطاعات الحكومية والخاصة في استخدام أجهزة الكمبيوتر وأنظمة المعلومات، وشبكات الأنترنت، والألواح الإلكترونية، والهواتف النقالة والذكية، وغيرها من تكنولوجيا المعلومات والاتصالات في إنجاز نشاطاتهم اليومية، تزايد معها احتمال تعرض الأفراد والمؤسسات والمجتمع إلى الهجوم من خلال استخدام تلك الوسائل، ولذلك تستمر العديد من دول وأقاليم العالم اليوم في السعي الجاد إلى تعزيز قوتها الإلكترونية والسيبرانية بهدف التقليل من المخاطر الأمنية الناتجة عن ذلك الاستخدام، وذلك بوضع وتطوير وتحسين استراتيجيات وسياسات وبرامج وتنظيمات قانونية تساعد في ضبط التحديات الناتجة عن الواقع الأمني الجديد الذي أفرزته البيئة الرقمية الراهنة والسيطرة عليها، وتعتبر ماليزيا إحدى دول العالم الثالث القليلة جدا التي كثفت جهودها في هذا المجال في وقت مبكر، كونها دخلت المجتمع المعلوماتي في وقت متزامن مع العديد من دول العالم المتقدم، حيث تم تصنيفها من قبل عدة خبراء وتقارير ودراسات في مراتب متقدمة نظرا للإنجازات التي حققتها حتى الآن للإندماج في مجتمع المعلومات.

فعلى مستوى إقليم آسيا والمحيط الهادي، احتلت ماليزيا المرتبة الأولى بين الدول الأكثر ذكاءا في المجال السيبراني وفقا لدراسة أجرتها شركة ESET [1] في 2015،[2] كما احتلت المرتبة الأولى أيضا في مؤشر نفاذ الأجهزة النقالة إلى الحزمة ذات النطاق العريض وفقا لتقرير قياس مجتمع المعلومات لسنة 2016 الصادر عن الاتحاد العالمي للاتصلات،[3] واعتبرت ماليزيا في نفس التقرير من بين الدول الخمسة الأولى في هذا الاقليم التي حققت أكثر ديناميكية في موشر تنمية تكنولوجيا المعلومات والاتصالات،4كما أنها احتلت المرتبة الثامنة في مؤشر تنمية تكنولوجيا المعلومات والاتصالات بقيمة قدرها 6.22 بعد أن كانت 5.64 في 2015،5 أما على المستوى الدولي، فقد احتلت سنة 2013 المرتبة الثانية عالميا فيما يتعلق بالنفاذ إلى حزمة النطاق العريض بعد روسيا في صنف الاقتصادات القائمة على الكفاءة في تصنيف ضم 26 دولة.6

وبالنسبة لخدمة الأنترنت، فقد دخلت إلى ماليزيا من قبل المعهد الماليزي للأنظمة الالكترونية الدقيقة The Malaysian Institute of Microelectronic Systems منذ سنة 1987، من خلال مشروع رانجكوم Rangkom الذي قام بربط عدة جامعات في ماليزيا بشبكة واحدة، وبعد نجاح هذه التجربة تم تحويل هذا المشروع سنة 1991 إلى مزود خدمة أنترنت يعرض خدماته على عدد محدود من العامة، وفي 1992 أطلق المعهد الماليزي للأنظمة الالكترونية الدقيقة أول مزود ماليزي لخدمات الانترنت سماه JARING 7 ويعني الشبكة، وتزايد عدد مزودي هذه الخدمة في ماليزيا تدريجيا إلى أن وصل الآن إلى 16 مزود.[8]

وتشير بعض الاحصائيات إلى أن عدد الأفراد المستخدمين لشبكة الانترنت في ماليزيا وصل سنة 2016 إلى أكثر من 21 مليون نسمة من عدد السكان البالغ عددهم ما يقارب 31 مليون نسمة،[9] كما تشير الأرقام الرسمية الصادرة عن دائرة الإحصاء التابعة للحكومة الماليزية سنة 2015 أن نسبة مستخدمي الأنترنت في ماليزيا وصلت إلى 71.1% من عدد السكان بينما شكلت نسبة استخدام الكمبيوتر 68.7% فيما شكلت نسبة استخدام الهاتف النقال97.5% من عدد السكان، وكان استخدام الأنترنت من ثلاثة أماكن رئيسية وهي من المنزل بنسبة 75% واثناء التنقلات بنسبة 72.2% ومن أماكن العمل بنسبة 41.5 %.[10]

وفي ظل هذه التحولات الرقمية التي يعيشها المجتمع الماليزي ودول كثيرة غيره، ظهر نوع جديد من التهديدات الأمنية التي تعتبر البيئة الرقمية إما سببا في نشأتها، أو عاملا مهما في انتشارها، وأصبحت تلك التهديدات تمس أمن الفرد والمؤسسات والمجتمعات المحلية والدول بل وعبرت حدود الدول، لتشكل بذلك تحديا آخرا تواجهه الدولة في سعيها لتحقيق أمنها الوطني أو القومي، ولا تعتبر ماليزيا استثناءا من هذا الوضع، ولذلك استمرت في تطوير سياسات وبرامج تساعدها في تعزيز قوتها وأمنها السيبرانيين، وذلك امتدادا لإستراتيجيتها الكبرى الشهيرة "رؤية 2020" والتي بدأتها الحكومة في 1991 وتعيش ماليزيا الآن في ظل خطتها الحادية عشرة والأخيرة (2016-2020).

وفي هذا السياق، تسعى هذه الورقة البحثية إلى تشخيص الواقع الأمني الجديد والسياسات الدفاعية الماليزية حياله، وتحديد ومناقشة التحديات التي تواجهها في ظل توسع وتنوع تلك التهديدات الأمنية، وذلك من خلال طرح التساؤلات التالية:

- ما المقصود بكل من سياسات الدفاع، البيئة الرقمية، القوة السيبرانية،الأمن السيبراني، والتهديد السيبراني؟

- ما هو الواقع الأمني الجديد الذي أفرزته البيئة الرقمية في المجتمع الماليزي؟ وكيف كيفت ماليزيا سياساتها الدفاعية لمواجهة التهديدات الأمنية الجديدة؟

- ماهي أهم التحديات التي لاتزال تواجه السياسات الماليزية في هذا السياق؟ وهل هناك تصورات حكومية للتقليل من أثرها السلبي على الأمن القومي الماليزي؟

وللإجابة على هذه التساؤلات، تم توظيف نظرية الأمننة لمدرسة كوبنهاغن، كما تم استخدام الأسلوب الكيفي كمنهج للبحث من خلال جمع وتحليل المعلومات الواردة في مختلف الوثائق والتقارير والتصريحات السياسية الرسمية والإعلامية التي صدرت عن مسؤولين ومؤسسات حكومية ماليزية ودولية، بالإضافة إلى تقارير لمؤسسات بحثية ومقالات وأبحاث منشورة لباحثين وخبراء ومختصين في هذا المجال.

وقد تناولت هذه الورقة البحثية أربعة نقاط أساسية، منطلقة من تحديد الإطار النظري والمفهوماتي للدراسة، ثم عرض للتهديدات السيبرانية والواقع الأمني الجديد في المجتمع الماليزي، ويليها تحليل ومناقشة السياسات الدفاعية الماليزية في مواجهة تحديات الأمن السيبراني، وصولا إلى التصورات الحكومية الماليزية حول سبل التقليل من الأثر السلبي لتلك التحديات على الأمن القومي الماليزي.

1- الخلفية النظرية والمفهوماتية للدراسة:

تمثل نظرية الأمننة أحد أهم التطورات في الدراسات الأمنية لتحليل النموذج الجديد للأمن الذي ظهر خلال الحرب على الإرهاب،[11]ففي عصر المعلومات اختلفت أنواع التهديدات الأمنية عن التهديدات التقليدية للأمن في نواح كثيرة، والأمر الأكثر وضوحا في هذا السياق هو الطريقة التي يتم من خلالها التصدي لهذه التهديدات الجديدة، حيث لا يمكن التصدي لها بالقوة الساحقة، ولا حتى من خلال بعض أنواع توازن القوى، وإنما من خلال شبكات معقدة من السياسات المتشابكة، فالحروب الجديدة لا تخاض وإنما تتم إدارتها. 12

فمفهوم الأمننة لمدرسة كوبنهاغن يمثل إطارا يمكنه أن يكون مثمرا من خلال دعواته إلى تحديد آليات أساسية خلف إعلان الأمن في مجموعة متنوعة من القطاعات، وتجدر الإشارة إلى أنه حتى الآن لم يتم استغلال إمكانيات هذا المفهوم التحليلية بشكل أمثل لاستكشاف الكيفية التي تتشكل من خلالها السياسات التي تحاول معالجة الظواهر الأمنية،13 فهذا المفهوم يصف عملية القيام بتحويل قضية معينة إلى نهاية أمنية ثم تقديمها بلغة أمنية، وهذه العملية في حد ذاتها تستدعي عدد من المفاهيم الأخرى، مثل "الموضوع المرجعي" referent object ويعني الشيء الذي يتم تهديده والذي يحتاج إلى الحماية، كالدولة والأمة وسيادتها والبيئية وغيرها، و"حركة الأمننة" securitizing move والتي تعني عملية تقديم قضية معينة باعتبارها "تهديدا وجوديا"existential threat للموضوع المرجعي المحدد، وهذه الحركة تتم من طرف الجهات الفاعلة في عملية الأمننة securitizing actor وتقدم إلى "الجمهور" audience.14

وقد تمت أمننة القضايا المرتبطة بتكنولوجيا المعلومات عموما في أواخر التسعينات، ووضع بعد ذلك هانسن Hansen و نيسنباوم Nissenbaum تصورا للأمن السيبراني كقطاع منفصل إلى جانب قطاعات الأمن الخمسة15 التي حددها باري بوزان وزملاؤه من قبل في مدرسة كوبنهاغن في إطار الدراسات الأمنية النقدية، وقطاع الأمن السيبراني يتميز بمجموعة مركبة من المسؤوليات في القطاعيين

العام والخاص والسلطة الحكومية، كما يتميز عن بقية القطاعات بالطريقة التي ترتبط من خلالها الموضوعات المرجعية المتمثلة في الفرد والشبكة بالأمن القومي أو أمن النظام والدولة.16

وتحاول هذه الورقة البحثية توظيف مفهوم الأمننة لمدرسة كوبنهاغن من خلال أمننة قضايا البيئة الرقمية والفضاء السيبراني بتشخيص التهديدات السيبرانية للدولة والمجتمع الماليزي، ومن خلال تحديد فواعل الأمننة المتمثلة في القطاعين الحكومي والخاص في مستوياته الدولية واللإقليمية والمحلية، بالاضافة إلى تحديد السياسات الحكومية الدفاعية الماليزية لمواجهة تلك التهديدات، ومن المهم قبل ذلك التطرق إلى بعض المفاهيم الأساسية للموضوع محل البحث، أهمها سياسات الدفاع، القوة السيبرانية، البيئة الرقمية، الأمن السيبراني، التهديدات السيبرانية.

فسياسات الدفاع Defense Policies: هو مفهوم استخدم في كثير من الأحيان كمرادف لمفهوم السياسات العسكرية، غير أن هذه الورقة البحثية تبنت مفهوما أوسع لسياسات الدفاع، والذي نظر إليها كسياسات تهدف إلى رسم وتطوير كافة الوسائل الكفيلة بتأمين الحفاظ على السيادة الوطنية، وهذه السياسة يتم تخطيطها وفقا لإدارة الحكام التي تحاول مواجهة كل خطر يهدد الدولة ومصالحها الحيوية،17 فأية سياسة دفاعية تعكس بالضرورة طبيعة النظام السياسي القائم وطبيعة العلاقة بين المدنيين والعسكريين في البلاد،18كما تبنت تعريف القاموس الحر الذي اعتبر السياسات الدفاعية عبارة عن برامج للدفاع عن البلد ضد أعدائه،19 ولم يحدد هذا التعريف طبيعة البرامج اسميا (عسكرية ام سياسية ام تقنية ام غيرها)، كما أنه لم يحدد نمط الأعداء (دول أم منظمات أم أفراد أو غير ذلك) لهذا يمكن اعتبارها كل ذلك، فمع تغير طبيعة التهديدات الأمنية الجديدة، والتي تتميز بكونها غير مرئية، وبالسرعة الشديدة في عبورها الحدود والأقاليم، لم يعد مفهوم سياسات الدفاع المقتصر على شقه العسكري وحده كافيا كأداة سياسية لمواجهة التحديات الأمنية لأي دولة، فقد أنتج هذا التغير حاجة إلى استخدام مفهوم سياسات الدفاع الموسع ليشمل مجالات مدنية عديدة إلى جانب المجال العسكري، ووفقا لهذا المفهوم الواسع فإن سياسات الدفاع ليس بالضرورة أن تكون ذات طبيعة عسكرية بالكامل، بل سياسات تشمل علاقة تعاونية وتكاملية مع الفواعل المدنية أيضا.

أما القوة السيبرانية Cyberpower: فهي تعني وفقا لتعريف قدمه دانيال كويل Daniel Kuehl في 2009 القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في جميع البيئات العملياتية وعبر أدوات القوة، ويقصد بالبيئات العملياتية المجالات الخمسة للقوة وهي، البرية، البحرية، الجوية، الفضائية، والفضاء السيبراني، بينما يقصد بأدوات القوة الأبعاد الأربعة للقوة وهي، الدبلوماسية، المعلومات، الجيش، والاقتصاد،20ويعد اعتبار القوة السيبرانية أحد الأبعاد المهمة للجيوبوليتكس Geopolitics أمرا طبيعيا ولا مفر منه، تماما مثل المجالات الاستراتيجية الأخرى،21 فرغم أن تأثير القوة السيبرانية يبقى الأقل ملموسية ووضوحا مقارنة بتأثير غيرها من أشكال القوة، كالقوة الجوية والبرية مثلا، إلا أنه في نفس الوقت لا يمكن اعتبار ذلك أمرا يقلل من أهميتها في الأمن السيبراني وفي مجال

نظريات الإستراتيجية،لأن انتشار القوة السيبرانية لا يمكن أن يلاحظ بشكل مباشر كون الأجهزة التي تولد نقل وتلقي المعلومات المتداولة، موجودة ماديا في كل مكان، كما أن المستفيدين المباشرين – والذين قد يكونون ضحايا في بعض الحالات– هم أيضا متواجدون في كل مكان،[22] وقد قدم جوزيف ناي وصفا للقوة السيبرانية يقول فيه بأنها تعتمد على الموارد التي يتميز بها مجال الفضاء السيبراني، وكونه ينظر إلى القوة على أنها القدرة على تحقيق النتائج المرجوة، فقد عرف القوة السيبرانية بأنها القدرة على تحقق النتائج المرجوة داخل الفضاء السيبراني، أو استخدام الأجهزة والأدوات في الفضاء السيبراني لتحقيق النتائج المرجوة في مجالات أخرى. [23]

وبالنسبة للبيئة الرقمية Digital Environment: فهي مفهوم ذو طبيعة كلية Macro label، وهو مرتبط بأي مجال للتفاعل البشري سهلته التكنولوجيا الرقمية، فموضوع البيئة الرقمية مجاله واسع جدا يشمل; الاتصالات الرقمية عن بعد بما فيها الخطوط الثابتة والنقالة، اتصالات الفاكس، البث الرقمي لوسائل الإعلام بمافيها الارضية والاقمار الصناعية، المنتجات الرقمية مثل الفيديو والموسيقى والصور، الأنترنت، برمجيات الحاسوب، برمجيات الألعاب، وسائل التتبع والأمن الرقمية، إدارة المعلومات أو قواعد البيانات، أدوات التوصيف الرقمية كتكنولوجيا توصيف الأوجه والتوصيف البيوميتري، وتكنولوجيا الأقمار الصناعية بمافيها GPS،[24] وتعتبر الأنترنت والتي يطلق عليها أيضا مصطلح الفضاء السيبراني Cyberspace مجرد مجال تعريف فرعي للبيئة الرقمية،[25]ويشير المختصون إلى أن تحديد مرجعية لحدود البيئة الرقمية هو أمر صعب جدا، لأن تلك البيئة متوسعة باستمرار.[26]

أما الأمن السيبراني Cyber Security: فرغم انتشار استخدامه غالبا كمصطلح متبادل مع مصطلح الأمن المعلوماتي Information Security، إلا أن عدة مختصين في مجال الأمن والكمبيوتر اعترفوا بالتداخل الشديد بين المصطلحين لكنهم في نفس الوقت أبرزوا أن المصطلحين ليسا متطابقين تماما، فالأمن السيبراني يتجاوز حدود الأمن المعلوماتي التقليدي ليشمل ليس حماية مصادر المعلومات فقط، بل كذلك أمن الأصول الأخرى بما فيها الشخص نفسه، وفي مجال الأمن المعلوماتي تتم الإشارة إلى العامل البشري عادة عندما يتعلق الأمر بدوره في العملية الأمنية، بينما في مجال الأمن السيبراني فهذا العامل له بعدا إضافيا، وهو أن البشر أهداف محتملة لهجمات إلكترونية أو حتى مشاركتهم دون درايتهم في تلك الهجمات، وهذا البعد الإضافي تترتب عليه آثار أخلاقية للمجتمع ككل، فحماية بعض الفئات الضعيفة كلأطفال مثلا، يمكن أن ينظر إليها باعتبارها مسؤولية اجتماعية.[27]

التهديدات السيبرانية Cyber threats: رغم أن التهديدات السيبرانية صعبة التحديد نظرا لسرعة نموها والتغير السريع لوسائلها إلا أن هناك عدة نماذج حاولت تحديدها، وأحد أهم تلك النماذج وأكثرها شيوعا هو ما يعرف بالتصنيف الخماسي fivefold classification الذي بني على أساس عوامل تحفيزية تدفعها الأنانية والفوضى والمال والتدمير والسلطة وتتمثل تلك العوامل فيما يلي:[28]

- الأنشطة السيبرانية: والتي تشمل كل من التخريب والقرصنة والنضال البرمجي، ويمكنها أن تتسبب في خسائر كبيرة للأفراد أو الشركات خصوصا مع تزايد نشاط المتسللين المجهولين بشكل اكثر فاعلية من الماضي.

- الجرائم السيبرانية: وهي الأعمال الإجرامية التي ترتكب باستخدام شبكات الإتصالات الإلكترونية ونظم المعلومات أو ضد هذه الشبكات والأنظمة.

- التجسس السيبراني: وهو الأفعال التي تهدف للحصول على معلومات سرية من الأفراد أو المنافسين أو المجموعات أو الحكومات أو الخصوم بهدف تحقيق مكاسب سياسية أو عسكرية أو اقتصادية عن طريق استخدام تقنيات غير مشروعة في الإنترنت، أو الشبكات، أو البرامج أو أجهزة الكمبيوتر.

- الإرهاب السيبراني: وهو استخدام الشبكات في الهجوم على نظم تكنولوجيات المعلومات والاتصالات الحساسة والتحكم بها، وتهدف تلك الهجمات لإحداث الضرر ورفع الخوف بين عامة الناس، ولإجبار القيادة السياسية لتحقيق مطالب الإرهابيين.

- الحروب السيبرانية: وتتكون من ثلاثة مكونات منفصلة وهي الحرب السيبرانية الإستراتيجية، الحرب السيبرانية التكتيكية والعملياتية، والحرب السيبرانية في النزاعات المنخفضة الحدة، ويستخدم مفهوم الحرب السيبرانية خاصة لوصف العمليات التي تقوم بها الجهات الفاعلة الدولتية في البيئة السيبرانية، وتتطلب الحرب السيبرانية حالة الحرب بين الدول مع إجراء العمليات السيبرانية كجزء من العمليات العسكرية الأخرى.

ومن خلال ما سبق يتضح أن الفضاء السيبراني لقي اعترافا أكاديميا وسياسيا وعسكريا بكونه قطاعا أمنيا ومجالا جيوبوليتيكيا وميدانا للحروب، حيث اعتبر وفقا لتطورات نظرية الأمننة لمدرسة كوبنهاغن أحد قطاعات الأمن ليضاف كقطاع سادس إلى القطاعات الخمسة المعروفة سابقا، كما أنه أضيف كمجال خامس للمجالات الأربعة المعروفة للقوة الجيوبوليتيكية، أما عسكريا فقد اعتبر وسيلة وميدانا للحروب الحديثة.

2- التهديدات السيبرانية والواقع الأمني الجديد في المجتمع الماليزي:

رغم أن النظرة العامة للأرقام الواردة في مقدمة هذه الورقة توحي بنمو سريع واتجاه إيجابي في مستوى اندماج ماليزيا في مجتمع المعلومات، إلا أن الصورة الكاملة لواقعها المعلوماتي تؤكد غير ذلك، فقد أوردت نفس الدراسة المذكورة سابقا، والتي أجرتها ESET في 2015 أن ماليزيا حققت لقب الدولة الأكثر قلقا على أمنها السيبراني،[29] كما أورد تقريرا للاتحاد العالمي للاتصالات صدر في 2015 بخصوص المؤشر العالمي للأمن السيبراني أن ماليزيا احتلت الرتبة الثالثة عالميا من حيث عدم الأمن السيبراني إلى جانبها كل من استراليا وسلطنة عمان بمؤشر قيمته 0.765 ويتصدرهم في هذا الموشر كل من الولايات المتحدة الأمريكية بقيمة 0.824 وكندا بقيمة 0.794.[30]

وتأتي التهديدات السيبرانية الناشئة عادة في أشكال مختلفة سواءا كانت تقنية أوذات علاقة بالمحتوى، وقد أصبحت اليوم أكثر تعقيدا وكارثية وشملت فاعلين حكوميين، وجهات فاعلة ترعاها دول، ومنظمات إجرامية دولية، ومجموعات القراصنة الناشطين على الأنترنت وغيرهم، فالتهديدات السيبرانية اليوم تضع تحديات أمام الحكومات والمنظمات والأفراد كما أن هناك اتجاها اليوم نحو الهجمات السيبرانية على البنيات التحتية الحيوية،[31]ويعترف الباحثون بهذا الخصوص أن هناك حضورا نشطا ومساهمة مهمة للفواعل غير الحكومية في الفضاء السيبراني، وأن تأثير هذه الفواعل في هذا الفضاء بات أكبر من تأثيرها في المجالات الأخرى، كما أشاروا إلى أنه يمكن للجهات الفاعلة غير الحكومية أيضا أن تلعب دورا كبيرا في الدفاع عن الحكومات الوطنية خلال الصراعات السيبرانية، وذلك بسبب ملكيتها وتشغيلها لعدة أنظمة وشبكات في القطاع الخاص،[32] وعادة تستخدم العديد من الأسلحة في التهديدات أو الهجمات السيبرانية أهمها الرموز والبرمجيات الخبيثة، والحرمان من الخدمة، والتهديدات ذات الصلة بالمحتوى، والبريد المزعج، والتحرش السيبراني والاحتيال والتسلل، وغيرها.

وهناك عدة عوامل تقود التغيير في البيئة الرقمية، أهمها الوقت،البيانات،التشبيك، والذكاء،[33] وبسبب سوء استخدام هذه البيئة، تزايدت بشكل كبير التهديدات الأمنية في العالم السيبراني، وأصبح هذا الفضاء لما يحتويه من مخاطرمن بين أكبر التهديدات التي تواجهها الدول، حيث اعتبرها البعض العدو غير المرئي لهم، كما أصبح من الصعب الكشف عن الجناة وراء تلك التهديدات، ونتيجة لذلك أصبح ينظر إلى البيئة الرقمية كميدان للحرب يهدد الأمن القومي والسيادة الوطنية.[34]

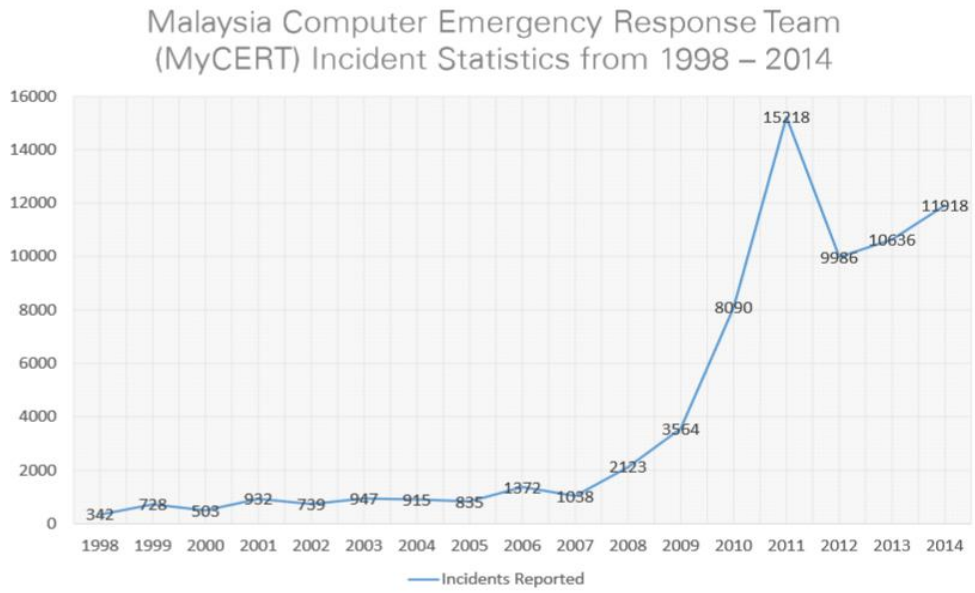
وبالنسبة للمجتمع الماليزي تحديدا، وبالإضافة إلى الإتجاهات الإيجابية والسلبية التي أوضحتها الأرقام السابقة فيما يتعلق بالبيئة الرقمية، نجد أن أغلب التهديدات الأمنية التي يواجهها الفرد، والمجتمع والدولة تتمحور في سوء استخدام وسائل التواصل الاجتماعي كالفايسبوك وتويتر والواتسآب وغيرها، بالاضافة الى انتشار الجريمة السيبرانية Cybercrime، الحرب السيبرانية Cyber warfare، التجسس السيبراني Cyber Espionage، والإرهاب السيبراني Cyber Terrorism، الأنشطة السيبرانية Cyber Activism.

فعلى الرغم من كون **وسائل التواصل الاجتماعي** موردا إستراتيجيا لا يقدر بثمن للدفاع والمجتمع العسكري، إلا أنه في كثير من الأحيان يشكل تهديدا للأمن الفردي والمجتمعي والقومي على حد سواء، ولأن ماليزيا تعتبر من أكثر المجتمعات استخداما لوسائل التواصل الاجتماعي في العالم،[35] ظهرت العديد من التهديدات الأمنية السيبرانية المرتبطة بسوء استخدام وسائل التواصل الاجتماعي في المجتمع الماليزي خاصة فيما يتعلق بمسألة خصوصية البيانات وما ينجم عنها من أضرار شخصية واقتصادية واجتماعية وحتى أمنية في حال سوء استخدامها.

فظاهرة التشبيك الاجتماعي تستهلك حياة ملايين المستخدمين في جميع أنحاء العالم، فمنذ انطلاق أول موقع للتواصل الاجتماعي، SixDegrees.com في 1997، نمت الشبكات الاجتماعية بشكل

كبير فاق كل التوقعات، وتعتبر خصوصية البيانات المشكلة الأساسية اليوم في عصر المعلومات، حيث يتم جمع كميات هائلة من البيانات من قبل الوكالات الحكومية، ومحركات البحث، وأنظمة التشبيك الاجتماعية، وقواعد تخزين البيانات في المستشفيات، والمؤسسات المالية، وغيرها من المنظمات، كل تلك المعلومات المخزنة أمر بالغ الأهمية بالنسبة للأفراد، وقد يسيء الناس استخدامها، تماما مثل المشاكل القائمة في العالم الحقيقي مثل السرقة والغش والتخريب وسرقات الهوية،[36]

وفي ما يتعلق **بالجرائم السيبرانية**، فقد تصاعدت إحصاءات الحوادث المسجلة حولها في ماليزيا بشكل دراماتيكي بين سنتي 1998 و2014 من 342 حادث إلى 11918 حادث، وسجلت أعلى ارتفاع لها سنة 2011 بتسجيل 15218 حادث وفق إحصاءات فريق استجابة طوارئ الكمبيوتر ماليزيا، كما يوضحه بالتفصيل الرسم البياني التالي:



Source: MyCERT Incident Statistics as of December 2014.

أما **الحرب السيبرانية** فتتضح من خلال تحويل النزاع الماليزي الفليبيني حول أراضي صباح المتنازع عليها إلى الفضاء السيبراني سنة 2013، حيث دار النزاع بين مجموعتين من قراصنة الأنترنت Hackers أحدهما عن الطرف الفلبيني سمى نفسه Philippine Cyber Army، والثاني عن الطرف الماليزي وهم ينتمون كما إدعو إلى Anonymous Malaysia.[37]

وبالنسبة **للتجسس السيبراني** فقد أصبح اليوم موضوعا مثيرا للنقاش أكثر من أي وقت مضى في جميع أنحاء العالم، وتصاعد الاهتمام به منذ تسريبات ويكيليكس من طرف جوليان أسانج Julian Assange في 2011 وكشفه عن برنامج PRISM [38]لإدوارد سنودن Edward Snowden في 2013، والمعلومات الحكومية ومعلومات عن الشركات وكذلك بيانات شخصية تم اعتراضها وأصبحت محورا لنشاط التجسس السيبران،[39]ومن أهم عمليات التجسس السيبراني الذي تعرضت له ماليزيا، هو ما عرضه تقرير شركة FireEye في أفريل 2015 حول مجموعة قراصنة يطلق عليهم اسم APT30

تستهدف الحكومات والشركات والصحفيين في جميع أنحاء جنوب شرق آسيا والهند وغيرها للحصول على معلومات استخباراتية حول القضايا السياسية والاقتصادية والعسكرية الإقليمية، مثل المطالبات الإقليمية المتنازعة حول بحر الصين الجنوبي بين الصين وماليزيا وغيرها من الدول، فماليزيا من الدول المستهدفة من هجمات سيبرانية مختلفة، بما في ذلك هجمات على الشبكات الحكومية الحساسة والسرية منذ 2005 على الأقل، وذكر نفس التقرير أن الجواسيس السيبرانيين استهدفوا دول الآسيان والتي تترأسهم ماليزيا اثناء اجتماعات آسيان الرسمية بهدف جمع معلومات حول السياسية والاقتصادية بالمنطقة.[40]

ورغم أن المعلومات حول **الإرهاب السيبراني** والإرهابيين السيبرانيين تعتبر غالبا معلومات سرية ولا يمكن الكشف عنها بسهولة للعامة، إلا أنه يمكننا استنتاج وجود هذا النوع من التهديد في ماليزيا من خلال بعض الأحداث التي وقعت وأربكت الحكومة الماليزية، مثل ما حدث في جوان 2011، بتعرض أكثر من 50 موقعا حكوميا ماليزيا للهجوم من قبل قراصنة، مما عطل عمل تلك المواقع، وهو ما جعل مسؤولون حكوميون يصرحون أن الأمة أصبحت أحدث هدف للحرب السيبرانية التي شنها ناشطون على الأنترنت،[41] وقد جاءت تلك الهجمات بعد تحذير جماعة تطلق على نفسها اسم "المجهول" Anonymous، والتي قالت انها ستهاجم البوابات الرسمية للحكومة لمعاقبتها على فرض رقابة على موقع ويكيليكس الذي يهدف إلى فضح الحكومات والشركات بتسريب وثائق سرية. [42]

فالسبب الرئيسي لانتشار الإرهاب السيبراني هو أن الإرهابي لا يحتاج إلى أي أداة متفجرة أو عالية التقنية للقيام بمهاجمة الضحية، فهو بحاجة فقط إلى نقل الفيروسات او البرامج الخبيثة أو سرقة أوتخريب أو تزوير المعلومات باستخدام التكنولوجيا الحالية مثل الهاتف، الكابل، أو الشبكة اللاسلكية، وهذا يساعدالارهابيين بالتأكيد ليكون أكثر مجهولية ويقلل من خطر وقوعهم في أيدي السلطات، ويمكن للإرهاب السيبراني أن يأتي في عدة أشكال وصور مثل: [43]

- مهاجمة انظمة الطاقة الكهربائية، إنتاج النفط والغاز، النقل، والتخزين، ونظم إمدادات المياه، النظم المالية والمصرفية.
- الوصول إلى منشآت صناعة الأدوية وتغيير صيغ الدواء لجعلها قاتلة.
- النفاذ الى سجلات المستشفيات وتغيير معلومات فصائل دم المرضى.
- الإعلان للآخرين عن معلومات مسروقة.
- التلاعب بالتصورات والآراء والتوجيه السياسي والاجتماعي والاقتصادي.
- تسهيل سرقة الهويات الشخصية.

وبالنسبة **للأنشطة السيبرانية**، فقد كان أهمها نشاطات حركة Persih "التنظيف"[44] التي تبنت استخدام وسائل الإعلام الرقمية منذ تأسيسها في 2006، وخلال السنوات التالية شهدت عملياتها في الوسائط الرقمية تطورا كبيرا، ففي البداية جعلت هذه الحركة من استخدام المواقع، والمدونات،

واليوتيوب كأدوات الرئيسية للتداول والتعبئة، مع استخدامات متقطعة لفليكر، وقد كان التدوين خيارا طبيعيا اضافة إلى إدماج يوتيوب وفليكر في 2006، والفيسبوك في 2008 وتويتر في 2011، الذي لم يكن مفاجئا في ظل شعبية هذه الأدوات بين الماليزيين وخاصة الشباب،[45]وقد نظمت حركة Persih 2.0 في جويلية 2011 حملة احتجاجية من أجل الإصلاح الديمقراطي في ماليزيا، استخدمت فيها بنطاق واسع الهواتف الذكية وشبكات التواصل الإجتماعية،[46] كما نجحت الحركة في عمل تجمع Persih 3.0 لـ 100000 شخص سنة 2012 والذي اعتبر أكبر تجمع احتجاجي في تاريخ ماليزيا الحديث،[47] وقد استمرت هذه الحركة في تنظيم التجمعات الاحتجاجية بالاستخدام الفعال للفضاء السيبراني والتي كان آخرها Persih 5.0 في أوت 2015.

3- الجهود والسياسات الدفاعية الماليزية في مواجهة تحديات الأمن السيبراني:

وفقا للمنظور الدفاعي الماليزي الذي جاء في وثيقة " سياسة ماليزيا للدفاع الوطني" فإن الهيمنة على مجال المعلومات هو أمر حاسم لحماية السيادة الوطنية، وأن تطبيق تكنولوجيا المعلومات والإتصالات أصبح أمرا لابد منه لضمان الهيمنة المعلوماتية على جميع المستويات والتي تشمل المستويات الاستراتيجية والتشغيلية والتكتيكية، فالتميز في تكنولوجيا المعلومات والاتصالات يعتبر ضمانا لتعزيز القدرة الدفاعية الوطنية وإضعاف قدرة العدو، وهي جهود تشمل بناء البنية التحتية وتطوير تطبيقات في هذا السياق.[48]

فلا بد من إعطاء الأولوية لتمكين جميع العناصر الدفاعية للبنية التحتية بوجودها في نظام شبكة اتصالات سلس، كما ينبغي أن يستكمل هذا الجهد بتطوير قاعدة بيانات مركزية تشرف عليها كل الوكالات التي تشارك في الدفاع عن السيادة الوطنية، ويتم دمج قاعدة البيانات هذه وتبادلها يكون من خلال عملية تشبيك مركزية للبنية التحتية، ووفقا لهذا المنظور فإن تطوير قدرات الحرب السيبرانية هي خطوة مهمة نحو موازنة قدرة البلدان الأخرى في المنطقة وكذلك للدفاع عن الأهداف الوطنية المستهدفة ضد جميع أشكال التهديد، ومهمة لوقف أي تعدي على أنظمة وشبكات الكمبيوتر التابعة للدفاع، وفي نفس الوقت يوفر أرضية لتطوير القدرات الهجومية لإجراء العمليات السيبرانية عند الضرورة. [49]

لقد حاولت الحكومة الماليزية منذ التسعينات تكييف سياساتها لتستجيب للتهديدات الجديدة المرافقة للبيئة الرقمية، وذلك من خلال التكامل الوظيفي بين الهيئات الحكومية ذات العلاقة بمسألة الأمن في سياق البيئة الرقمية، مثل وزارة الدفاع ووزارة العلوم والتكنولوجيا والابتكار، والمجلس الوطني لتكنولوجيا المعلومات وغيرها، كما انشأت العديد من السياسات والبرامج خاصة السياسة الوطنية للأمن السيبراني والأمن السيبراني ماليزيا، والحضيرة الماليزية لتكنولوجيا الدفاع، ومبادرات اخرى سترد لاحقا، كما وسعت الحكومة الماليزية دائرة التعاون في هذا المجال مع القطاع الخاص، ووضعت عددا مهما من التنظيمات القانونية بهدف تعزيز أمنها السيبراني سميت بالقوانين السيبرانية.

فوزارة الدفاع الماليزية عملت على تطبيق **السياسة الأمنية لتكنولوجيا المعلومات** بهدف حماية الحكومة والشركات من أي هجوم سيبراني، وكان من بين مهامها ضمان سلامة الشبكات ومنع الحوادث السيبرانية من إحداث آثار إقتصادية مدمرة.[50]

ووزارة العلوم والتكنولوجيا والابتكار الماليزية (MOSTI) قامت في 2005 بإجراء دراسة حول **السياسة الوطنية للأمن السيبراني (NCSP)** والذي أقرته الحكومة كسياسة واضحة فيما بعد في ماي 2006، وتمت صياغة تلك السياسة لمواجهة التهديدات والمخاطر التي تتعرض لها البنية التحتية الوطنية الحساسة للمعلومات (CNII) وكذلك لتطوير خطط عمل لتخفيف تلك المخاطر، وتكونت هذه السياسة من ثمانية محاور او توجهات أساسية هي: الحوكمة الفعالة، الإطار التشريعي والتنظيمي، إطار تكنولوجيا الأمن السيبراني، ثقافة الأمن وبناء القدرات، البحوث والتنمية نحو الاعتماد على الذات، الالتزام والإنفاذ، الاستعداد لحالات طوارئ الأمن السيبراني، والتعاون الدولي[51]

والبنية التحتية الوطنية الحرجة للمعلومات هي عبارة عن مجموعة من الأنظمة والوظائف تعتبر حيوية للدول ويكون لاستغلالها أو لتلفها أو لتدميرها تأثير مدمر جدا على القوة الاقتصادية الوطنية، والدفاع والأمن، وقدرات الحكومة على العمل بكفاءة، وعلى الصحة العامة والسلامة، وتركز السياسة الوطنية الماليزية للأمن السيبراني بشكل خاص على حماية تلك البنية التحتية ضد التهديدات السيبرانية، وتوفر آليات لتحسين الثقة والتعاون بين القطاعين العام والخاص، كما تدعم هذه السياسة الشركاء والحلفاء الدوليين في ماليزيا، وتصف الأساليب التي يمكن لماليزيا من خلالها تبادل المعرفة مع دول المنطقة والعالم فيما يتعلق بمسائل الأمن السيبراني، فتطوير هذه السياسة الوطنية جاء كخطوة استباقية لحماية القطاعات الحيوية ضد التهديدات السيبرانية.[52]

في سنة 2007 تم إطلاق برنامج **الأمن السيبراني ماليزيا Cybersecurity Malaysia** [53]من طرف رئيس الوزراء في اجتماع للمجلس الوطني لتكنولوجيا المعلومات، والأمن السيبراني ماليزيا هي وكالة وطنية تابعة لوزارة العلوم والتكنولوجيا والابتكار (MOST)، وتشرف على ادارة مركز لمساعدة مستخدمي الإنترنت، ومركز للتدريب المهني، وتعمل أيضا على تزويد الجمهور بمعلومات عن التهديدات السيبرانية، كما تشارك الوكالة في مجال إنفاذ قوانين مكافحة الجريمة السيبرانية خاصة بعد الهجمات ضد المواقع الحكومية في 2011. [54]

أما **الحضيرة الماليزية لتكنولوجيا الدفاع"MDSTP" Malaysia Defence Technology Park** ، التي تعد وفق تصريح وزير الدفاع الماليزي زاهد حميدي Zahid Hamidi الأولى من نوعها في منطقة آسيان لتلبية الطلب واحتياجات الصناعة الدفاعية والأمنية المتزايدة،[55] فهي تستهدف ثلاثة قطاعات أساسية هي القطاع الجوي والقطاع البحري وقطاع السيارات،[56] وتسعى هذه الحضيرة إلى تحقيق مجموعة من الأهداف تتمثل في:[57]

– دفع ماليزيا إلى اقتصاد يقوده الابتكار، من خلال استضافة مراكز البحث والتنمية الأكثر تطورا وتكاملا، وإنتاج منتجات الصناعة الدفاعية بشكل مبتكر.

– تسهيل الأبحاث الدفاعية والتطوير والابتكار وأنشطة التسويق من خلال توفير بنية تحتية ومعدات ومرافق متطورة.

– تشجيع تطوير بيئة مواتية لمنتجات وتكنولوجيا الدفاع الفكرية والإبداعية والمبتكرة.

– تسهيل الشراكات الذكية بين القطاعين الحكومي والخاص في تطوير تكنولوجيا الدفاع وتسويق نتائج البحوث.

– إعداد مقدمي الصناعة الدفاعية المحليين للمشاركة في عقد مناقصة عالمية.

– تمكين مقدمي الصناعة الدفاعية المحلية والدولية من تصنيع المنتجات للسوق المحلي والإقليمي والعالمي.

وهناك أيضا **فريق الاستجابة لطوارئ الكمبيوتر ماليزيا Malaysia Computer Emergency Response Team (MyCERT)** والذي يعود انشاؤه إلى 1997، ويعمل الآن من مكتب الأمن السيبراني ماليزيا، ويقدم نقطة مرجعية لمجتمع الإنترنت في ماليزيا للتعامل مع حوادث أمن الكمبيوتر، كما يوفر المساعدة في معالجة حوادث مثل التسلل وسرقة الهوية، وعدوى البرامج الخبيثة والتحرش السيبراني وغيرها من الحوادث المتعلقة بأمن الكمبيوتر، ويعمل MyCERT بشكل وثيق مع وكالات إنفاذ القانون مثل الشرطة الملكية الماليزية، الهيئات الأمنية ، وبنك نيجارا ماليزيا (البنك المركزي)، وله أيضا تعاون وثيق مع مقدمي خدمة الإنترنت (ISP)، وفرق الاستجابة لحوادث أمن الكمبيوتر، ومختلف المبادرات أمن الكمبيوتر في أنحاء مختلفة من العالم،[58] ويسهر على مركزين أحدهما مخصص لمساعدة مستخدمي الأنترنت في ماليزيا، والثاني لإجراء أبحاث البرمجيات الخبيثة.

فمركز أبحاث البرمجيات الخبيثة، أطلقته الأمن السيبراني ماليزيا في ديسمبر 2009، ويعمل هذا المركز على انجاز شبكة بحوث لتحليل البرامج الخبيثة و التهديدات التي تواجه أمن الكمبيوتر، وقد أنشأ المركز أيضا تعاونا مع الباحثين والأطراف الموثوقة لتبادل المعلومات البحثية. [59]

ويقدم **مركز المساعدة Cyber999** التابع للأمن السيبراني ماليزيا خدمة لمستخدمي الإنترنت اطلق عليها Cyber999 لتقديم شكاوى أو تقارير حوادث أمن الكمبيوتر، ويتم الإعلام بتلك الحوادث عبر ستة طرق وهي، عن طريق نموذج متوفر على الانترنت، أو من خلال إرسال بريد إلكتروني، أو إرسال رسالة نصية SMS، أو الاتصال عبر الهاتف، او عن طريق الفاكس، او من خلال تطبيقات الهاتف المحمول.[60]

وفي مجال التشريعات والقوانين السيبرانية Cyber Laws فهناك عدة قوانين وتنظيمات تبنتها ماليزيا للتعامل مع تهديدات البيئة الرقمية المختلفة، أهمها كان قانون التوقيع الإلكتروني وقانون جرائم الكمبيوتر وقانون حقوق التأليف وقانون الطب عن بعد وكلها كانت في1997، قانون الاتصالات

والوسائط المتعددة في1998، قانون الاقراص الضوئية في 2000، وقانون أنظمة الدفع في 2003، وقانون التجارة الإلكترونية في 2006، وقانون أنشطة الحكومة الالكترونية في 2007 وقانون حماية البيانات الشخصية في 2010، وقانون خدمات البريد 2012، وقانون العقوبات.[61]

4- الآفاق الاستراتيجية للدفاع والأمن السيبرانيين في ماليزيا:

لقد أنشأت القوات المسلحة الماليزية في 2015 **وحدة خاصة بالدفاع السيبراني** لحماية المعلومات السرية حول أنظمة الدفاع من الاختراق والتسريب، وأعلن وزير الدفاع الماليزي هشام الدين حسين في أواخر شهر اوت 2016 بعد تسرب بيانات سرية حول غواصات سكوربين الفرنسية الصنع، أن هذه الوحدة تراقب عن كثب الأنشطة السيبرانية التي تشكل تهديدا محتملا للنظام الدفاعي للبلاد، كما أنها تعمل من أجل تعزيز نظام الدفاع السيبراني، وإجراء تدقيق للوضع الأمني وكذلك الأدلة الجنائية السيبرانية، وذكر وزير الدفاع أنه تم إنشاء هذه الوحدة الخاصة بالدفاع السيبراني تحت إشراف شعبة الاستخبارات لأركان الدفاع،[62]والتي تمثل وكالة الاستخبارات العسكرية للقوات المسلحة الماليزية، كما أكد أن هناك عدة محاولات كانت فاشلة لاختراق أسرار عسكرية للبلاد تخضع لحراسة مشددة،[63] كما صرح أن ماليزيا تقوم بضبط نظام دفاع سيبراني متطور، اكتمل منه 90% حتى الآن بعد ثلاث سنوات من العمل.[64]

وذكر الرئيس التنفيذي لوكالة الأمن السيبراني ماليزيا، أمير الدين عبد الوهاب في 2016، أن الوكالة لديها عدة معالم رئيسية للوصول إليها بحلول عام 2020، والهدف هو عولمة ماليزيا للأمن السيبراني وتوسيع والانخراط في مبادرات من خلال التعاون الثنائي والمتعدد الأطراف مع الوكالات المحلية والدولية لتعزيز استراتيجيات الأمن السيبراني في البلاد.[65]

وتشير بعض التقارير إلى أن القوات المسلحة الماليزية قد بدأت في تطوير قدراتها لحماية الأصول الوطنية، من التهديدات السيبرانية، كما أعلن وزير الدفاع الماليزي تأييده لوضع خطة آسيان الرئيسية للأمن السيبراني في جنوب شرق آسيا، وهو مايعكس إدراك المخاطر والتهديدات السيبرانية داخل القوات المسلحة الماليزية،[66] وفي مجال **التعاون الدولي والثنائي**، تعمل ماليزيا من خلال فريق استجابة طوارئ الكمبيوتر ماليزيا(**MyCERT**)، على تنسيق جهودها في ظل التعاون الدولي مع منظمة آسيان من خلال ASEAN CERT ، ومع دول مؤتمر التعاون الاسلامي من خلال OIC-CERT ، ومع دول آسيا والمحيط الهادي من خلال APCERT والتي تعتبر عضوية ماليزيا فيها كنائب لرئيس هذا التعاون للفترة الممتدة من سبتمبر 2015 إلى سبتمبر 2017،[67] كما عملت الشرطة الماليزية في 2015 على التعاون مع الأنتربول والاف بي أي FBI لتتبع الاشخاص الذين انخرطوا في تهديدات الحروب السيبرانية التي تبنتها Anonymous Malaysia وقد تم توقيفهم اثناء محاولتهم التخطيط لهجمات وفق حمزة طيب نائب مدير القسم الفدرالي للتحقيق في الجرائم التجارية،فقد نشرت Anonymous Malaysia سابقا فيديو في صفحتها على الفايسبوك فيديو مدته ثمانية دقائق تدعو فيه لاستقالة الرئيس الماليزي.[68]

أما على مستوى **التعاون المحلي بين القطاعين العام والخاص**، فقد قامت وزارة العلوم والتكنولوجيا والابتكار في سبتمبر 2016 بالاعلان عن مشروع أسمته **نطاق ماليزيا السيبراني** cyber Range Malaysia وهو عبارة عن بيئة افتراضية تستخدم لتطوير التكنولوجيا السيبرانية بالاضافة إلى التدريب على الحرب السيبرانية، وتم تطوير هذا المشروع في اطار التعاون بين القطاعين العام والخاص وهو يستهدف تدريب 10000 محترف في الأمن السيبراني بحلول سنة 2020، ويطمح هذا المشروع إلى دفع المدافعين السيبرانيين لحماية شبكات المنظمات والشركات في ماليزيا، من خلال توفير التدريب والخدمات في هذا المجال بهدف تحقيق الاعتماد على الذات.[69]

وبالإضافة إلى التعاون والشراكات على المستويات الدولية، الإقليمية، والمحلية، لا تزال الحكومة الماليزية مستمرة في تكثف جهودها التي تهدف إلى رفع مستوى الوعي الأمني السيبراني لدى مواطنيها من خلال وكالة الأمن السيبراني ماليزيا، وبالنسبة للأنشطة المستقبلية لهذه الوكالة فهي مهتمة بإنتاج المحتوى ابتكاري وذو صلة بالجمهور المستهدف، وتشجيع الشراكات بين القطاعين العام والخاص، وقياس فعالية الحملات التي تجرى في هذا المجال.[70]

وقد نظم **مجلس الأمن القومي (NSC) بالتعاون مع وكالة الأمن السيبراني ماليزيا** ورشة عمل في جانفي 2015 لمناقشة وضع **الخطة الرئيسية للتوعية الوطنية حول الأمن السيبراني** National Cyber Security Awareness Master Plan، وحضر هذه الورشة 19 منظمة من مختلف الوزارات والوكالات الحكومية والمنظمات غير الحكومية وممثلي الشركات الخاصة التي تشارك بشكل مباشر في تعزيز الوعي الأمني السيبراني في ماليزيا، وتسعى ماليزيا من خلال امتلاك الخطة الرئيسية الوطنية للتوعية حول الأمن السيبراني (CSA)، لوضع ماليزيا كدولة رائدة لحملة التوعية حول الأمن السيبراني في العالم.[71]

الخاتمة

إن واقع التهديدات الأمنية في الفضاء السيبراني في ماليزيا لا يختلف كثيرا عن واقعها في بقية الدول المندمجة في المجتمع الرقمي والمعلوماتي، بما في ذلك الدول الفائقة التطور في مجال تكنولوجيا المعلومات والإتصالات، ويتضح من خلال كل ما سبق أن البيئة الرقمية رغم أنها حملت معها الكثير من الإيجابيات على مستويات عديدة وخاصة المستوى الإقتصادي، إلا أنها في المقابل فرضت تهديدات أمنية سيبرانية للفرد والمجتمع والدولة والنظام على حد سواء، تجاوزتأثيرها الحدود الجغرافية والطبيعية للدول، هذا بالإضافة إلى توسع وتنوع الفاعلين في هذا المجال، فالجريمة، والإرهاب، والجوسسة، والقرصنة، والحروب أصبحت في البيئة الرقمية أكثر انتشارا وفاعلية من قبل، كما أن الناشطين في هذا المجال أصبحوا أكثر قدرة على التخفي وبالتالي أقل تعرضا للتعقب في حالات ارتكاب هجماتهم السيبرانية المتنوعة الدوافع، لذلك حاولت ماليزيا – مثل غيرها من الدول التي تواجه هذا النوع من التحديات الأمنية– تكييف سياساتها الدفاعية مع النمط الجديد لهذه التهديدات، فرغم أن

الهدف الأول والأساسي لسياسات الدفاع الوطني في ظل هذه البيئة يبقى الحفاظ على سيادة الدولة القومية وحماية مصالحها، إلا أن الحكومة الماليزية أدركت بوضوح بأن نجاعة تلك السياسات لا يمكنها أن تتحقق بانفراد الدور الحكومي في هذا المجال، ولذلك تبنت سياسات دفاعية تتماشى مع هذا الواقع الجديد من خلال فتحها لمجال التعاون والشراكات بين القطاعين العام والخاص، وتكثيف الجهود على المستويات الدولية والثنائية والمحلية.

ورغم أن ماليزيا تعتبر تاريخيا وإحصائيا من الدول ذات الخبرة المعتبرة في مسارها لترقية مجتمعها نحو مجتمع رقمي، ثم معلوماتي، وتستمر الآن في طموحها نحو مجتمع معرفي، إلا أن تلك الخبرة كما توصلت إليه هذه الورقة لم تكن ضمانا كافيا لحماية أمن الأفراد والمجتمع وبالتالي الأمن القومي من الآثار الأمنية السلبية للبيئة الرقمية، وهذه المعضلة تواجه الآن أغلب المجتمعات التي انتقلت نشاطات أفرادها ومؤسساتها وحكوماتها إلى الفضاء السيبراني، وهو ما جعل اهتمام الدول الذكية اليوم هو ابتكار طرق وكيفيات تعزيز من القوة السيبرانية Cyberpower كإحدى استراتيجيات تحقيق الأمن القومي والمصالح القومية، وهذا ما يدعونا إلى طرح إشكاليات أخرى، تتعلق بمدى تناسب المجهودات الماليزية المختلفة في سن سياساتها الدفاعية السيبرانية مع تحقيق أمنها القومي حتى الآن، وكيف يمكنها كدولة ناشئة أن تعزز من قوتها السيبرانية؟ خاصة في ظل تسارع دول كبرى مثل الصين والولايات المتحدة الأمريكية نحو الهيمنة على هذا النمط الجديد من القوة وتنافسها بهدف تعزيز قوتها للتموقع دوليا أو للحفاظ على موقعها الدولي في العالم السيبراني الذي يعتبر امتدادا لمواقعها في العالم الحقيقي.

الهوامش :

1. وهي شركة رائدة في مجال الحماية الاستباقية في مجال التكنولوجيا، تعمل لأكثر من 26 سنة كمزود عالمي للحلول الامنية للشركات والمستهلكين الافراد، مثل الكشف عن عمليات الاختراق ومكافحة الفيروسات وغيرها من التهديدات الامنية للفضاء السيبراني.
2. ESET.*" ESET Asia Cyber-Savviness Report 2015: Cyber Security : User Knowledge, Behavior and Attitudes in Asia",* (2015), p5, Retrieved on 17/12/2016 from: https://static1.esetstatic.com/fileadmin/Images/SG/Images/Files/ESET%20Asia%20Cybersavviness%20Report%202015.pdf
3. International Telecommunication Union (ITU). *"Measuring the Information Society Report 2016"*, Switzerland, Geneva, (2016), p57, Retrieved on 17/12/2016 from: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf
4. Ibid., P58.
5. Ibid., p 56.
6. Neville, Spykerman. *"Malaysia second in world broadband penetration ranking"* the star online, 28 October 2013, Retrieved on 17/12/2016 from: http://www.thestar.com.my/news/nation/2013/10/28/broadband-penetration-muhyiddin-yassin/
7. Ali, Salman. & Mohd Safar, Hasim. "Internet Usage in a Malaysian Sub-Urban Community: A Study of Diffusion of ICT Innovation" *The Innovation Journal: The Public Sector Innovation Journal*, Vol 16, N 2,(2011), p 2, Retrieved on 17/12/2016 from:

http://www.innovation.cc/case-studies/salman%20hasim_internet_usage_sub-urban_community5rvsd1final_v16i2a8.pdf

8. ISP. *" ISP List In Malaysia"*, Retrieved on 17/12/2016 from: http://isp-in-malaysia.blogspot.com/2011/04/isp-listing.html

9. Internet live stats, *" Malaysia Internet Users (2016)"* , Retrieved on 17/12/2016 from: http://www.internetlivestats.com/internet-users/malaysia/

10. Official Portal of Department of Statistics Malaysia, *"ICT Use and Access by individuals and households survey Report Malaysia 2015"*, Retrieved on 17/12/2016 from: https://www.statistics.gov.my/index.php?r=column/cthemeByCat&cat=395&bul_id=Q3l3WXJFbG1PNjRwcHZQTVlSR1UrQT09&menu_id=amVoWU54UTl0a21NWmdhMjFMMWcyZz09

11. Jonathan, Bright. "Security, Technology and Control: Repositioning Securitisation Theory for the Information Society", Paper presented at *"Politics in Hard Times: International Relations Responses to the Financial Crisis"* SGIR 7th Pan-European Conference, Stockholm, September (2010), P1, Retrieved on 27/12/2016 from: http://www.eisa-net.org/be-bruga/eisa/files/events/stockholm/Security,%20Technology%20and%20Contol%20-%20%20J%20Bright%20-%20SGIR%202010.pdf

12. Ibid,. P3.

13. Ibid,.

14. Ibid,. p4.

15. [1] القطاعات الخمسة هي: القطاع السياسي، القطاع العسكري، القطاع الاقتصادي، القطاع المجتمعي، القطاع البيئي.

16. Thierry, Balzacq et al. " Securitization revisited: Theory and Cases", *International Relations*, Vol 30 N 4, (2016), pp 516-517, Retrieved on 27/12/2016 from: http://journals.sagepub.com/doi/pdf/10.1177/0047117815596590

17. دلال محمود السيد محمود، *" الاستمرارية والتغير في السياسة الدفاعية الإسرائيلية: دراسة مقارنة لما بعد حربي اكتوبر 1973 ويونيو 2006"* الجزء الاول، مصر القاهرة:المكتب العربي للمعارف، 2015، ص23.

18. مركز دراسات الجزيرة، *"واقع وآفاق السياسات الأمنية والدفاعية بالعالم العربي " تم الاطلاع بتاريخ:*2017/01/03، على الرابط: http://anntv.tv/new/showsubject.aspx?id=19384

19. The Free Dictionary, *"Defense Policy"*, Retrieved on 27/12/2016 from: http://www.thefreedictionary.com/defence+policy

20. Jill, Rowland et al. "The anatomy of a cyber power", *international journal of critical infrastructure protection*, 7, (2014), p 7.

21. John B, Sheldon. "Geopolitics and Cyber Power: Why Geography Still Matters", *American Foreign Policy Interests*, Vol 36, N 5, (2014), p 287.

22. Ibid,.

23. Jill Rowland et al, (2014), Op.cit.

24. Andrew, Murray. "*The Regulation of Cyberspace: Control in the Online Environment*", Taylor and Francis Group, Routledge- Cavendish: USA and Canada, (2007), p59.

25. Ibid.

26. Ibid,. p60.

27. Rossouw von, Solms. & Johan van, Niekerk. "From information security to cyber security", *computers & security*, xxx, (2013), p1. Retrieved on 27/12/2016 from: http://www.sciencedirect.com.sci-hub.cc/science/article/pii/S0167404813000801

28. Martti Lehto Pekka Neittaanmäki, *"Cyber Security: Analytics, Technology and Automation"*, Springer: New York, London, Switzerland, (2015),p 9.

29. ESET,(2015), Op.cit., P7.

30. International Telecommunication Union (ITU), *"Global Cybersecurity Index & Cyberwellness Profiles"*, ITU: Switzerland, Geneva, (2015), p1.

31. Amirudin, Abdul Wahab. *"Cyber Security as a Central Strategy for Smart Community"*, Proceedings of the 4 th International Conference on Computing and Informatics, ICOCI 2013 28-30 August, (2013) Sarawak, Malaysia. Universiti Utara Malaysia, Retrieved on 27/12/2016 from: http://www.icoci.cms.net.my/proceedings/2013/PDF/Keynotes%201.pdf

32. Jill Rowland et al, (2014), Op.cit,.

33. Martti Lehto Pekka Neittaanmäki,(2015), Op.cit., p7.

34. Ainaa Nadzirah, Binti Malek Farok. " *Cyberspace as a National Security Issue in Malaysia",* a dissertation submitted in fulfillment of the requirement for the degree of Master of Political Science, Kulliyyah of Islamic Revealed Knowledge and Human Science, International Islamic University Malaysia, (2015), p7.

35. Lalitha, Muniandy. & Balakrishnan, Muniandy. "The Impact of Social Media in Social and Political Aspects in Malaysia: An Overview", *International Journal of Humanities and Social Science*, Vol 3 No. 11, (2013), p 75, Retrieved on 27/12/2016 from: http://www.ijhssnet.com/journals/Vol_3_No_11_June_2013/8.pdf

36. Aida, Abdulahi et al. "A Study on the Negative Effects of Social Networking Sites Such as Facebook among Asia Pacific University Scholars in Malaysia", *International Journal of Business and Social Science*, Vol 5, No 10, (2014), p136, Retrieved on 27/12/2016 from: http://ijbssnet.com/journals/Vol_5_No_10_September_2014/18.pdf

37. Mohit, Kumar. *"Philippines-Malaysia Cyber war over Sabah land dispute*" , the Hacker News: Security in serious way, Retrieved on 27/12/2016 from: http://thehackernews.com/2013/03/philippines-malaysia-cyber-war-over.html

38. [1] هو برنامج أمريكي للمراقبة الإلكترونية من خلال جمع المعلومات من شبكة الإنترنت وغيرها من مقدمي الخدمات الإلكترونية.

39. Zahri, Yunos. & Zaleha, Abd Rahim. *"Cyber espionage: The rise of threats in the cyber dimension"* Computerworld Malaysia, Retrieved on 27/12/2016 from: http://www.computerworld.com.my/blogs/guest-blogs/guest-insight-cyber-espionage-the-rise-of-threats-in-the-cyber-dimension/

40. MalayMail online, *"China hackers spying on Malaysia, says report"*, MalayMail online, April 13, 2015, Retrieved on 27/12/2016 from: http://www.themalaymailonline.com/malaysia/article/china-hackers-spying-on-malaysia-says-report#sthash.e9hgoge0.dpuf

41. Liau, Y-Sing. &Niluksi, Koswanage. *"Hackers disrupt 51 Malaysian government websites",* Reuters, 16 Jun 2011, Retrieved on 27/12/2016 from: http://www.reuters.com/article/us-malaysia-hackers-idUSTRE75F06Y20110616

42. Ibid,.

43. Jian, Hua & Sanjay, Bapna. "The economic impact of cyber terrorism", *Journal of Strategic Information Systems*, 22 , (2013), p 177.

44. [1] هي حركة تعتبر نفسها حركة مجتمع مدني غير حزبية، غير أن أهم مؤيديها هم الأحزاب الرئيسية الثلاثة المعارضة Malaysian Islamic Party (PAS), Democratic Action Party (DAP) and Parti Keadilan Rakyat (PKR)، وهي تشكل مع بعض التحالف المعارض Pakatan Rakyat (PR).

45. Merlyna, Lim. "Sweeping the Unclean: Social Media and the *Bersih* Electoral Reform Movement in Malaysia", *Global Media Journal*, Vol 14, N 27, 2016, Retrieved on 27/12/2016 from: https://www.globalmediajournal.com/open-access/sweeping-the-unclean-social-media-and-the-bersih-electoral-reformmovement-in-malaysia.php?aid=83245

46. Postill, John. " A critical history of internet activism and social protest in Malaysia, 1998-2011", *Asiascape: Digital Asia Journal* Vol 1 N1-2, 2014, Retrieved on 27/12/2016 from: http://booksandjournals.brillonline.com/content/journals/10.1163/22142312-12340006
47. Malaysiakini, "*Hacktivist attack will jeopardise Bersih 4*", Malaysiakini,12/08/2015, Retrieved on 27/12/2016 from: http://www.malaysiakini.com/news/308280
48. Ministry of Defence (MOD), *"Malaysia's National Defence Policy",* pp12-13, Retrieved on 27/12/2016 from: http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf
49. Ibid., p13.
50. James A, Lewis. & Katrina, Timlin. *"Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization"*, Center for Strategic and International Studies, (2011), Retrieved on 27/12/2016 from: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf
51. Zahri, Yunos.& Syahrul, Hafidz. *"Cyber Terrorism And Terrorist Use Of ICT And Cyberspace"*, Retrieved on 27/12/2016 from: http://www.searcct.gov.my/featured-articles/49-cyber-terrorism-and-terrorist-use-of-ict-and-cyberspace
52. [1] Ibid,.
53. كانت CyberSecurity Malaysia تعرف قبل ذلك في 1997 National ICT Security and Emergency Response Center
54. James A, Lewis. & Katrina, Timlin.(2011), Op.cit,.
55. Malaysian Defence Technology Park (MDSTP), Retrieved on 27/12/2016 from: http://mdstp.com.my/home/
56. Ibid,.
57. Blenheim Capital Partners Limited, *"Blenheim Capital to support Malaysia Defence & Security Technology Park",* Retrieved on 27/12/2016 from: http://www.blenheimcapital.net/downloads/Blenheim_Capital_to_support_Malaysia_Defence_Security_Technology_Park_-_20_July_2010.pdf
58. MyCERT, *" About Us"* Retrieved on 27/12/2016 from: https://www.mycert.org.my/en/about/about_us/main/detail/344/index.html
59. MyCERT, *" Cyber999 Help Center",* Retrieved on 27/12/2016 from: https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/443/index.html
60. MyCERT, " *CyberSecurity Malaysia Malware Research Centre",* Retrieved on 27/12/2016 from: https://www.mycert.org.my/en/services/malware_research/about/main/detail/761/index.html
61. Amirudin, Abdul Wahab. *"Evolving Threats of Cyber Crime and How to Stay Ahead– Malaysia's Experience"*, (2015), p13, Retrieved on 27/12/2016 from: http://www.vipforum.ru/upload/iblock/13b/13b483033bc042a01586ed37478abb45.pdf
62. ترفع هذه الشعبة تقارير إلى قائد القوات المسلحة، وإلى وزير الدفاع، وإلى شعبة الأمن القومي.
63. Adrian, Lai. *"Armed Forces set up cyber defence unit last year to prevent info leakage, hacking"*, New Straits Times Online, 28 August (2016), Retrieved on 27/12/2016 from: http://www.nst.com.my/news/2016/08/168808/armed-forces-set-cyber-defence-unit-last-year-prevent-info-leakage-hacking
64. Prashanth, Parameswaran. *"Malaysia's Cyber Defense: One of ASEAN's Best?",* the diplomat, 26 October (2016), Retrieved on 27/12/2016 from: http://thediplomat.com/2016/10/malaysias-cyber-defense-one-of-aseans-best/

65. Ahmad, Kushairi. *"Raising the alert on cybersecurity"*, New Srtaits Times Online, 2 November(2016), Retrieved on 27/12/2016 from: http://www.nst.com.my/news/2016/11/185226/raising-alert-cybersecurity

66. International Cyber Policy Center, *"Cyber Maturity in the Asia- Pacific Region 2014"*, Australia: Australian Strategic Policy Institute, (2014), p34.

67. Asia Pacific Computer Emergency Response Team (APCERT). *" APCERT Annual Report 2015",* p170, Retrieved on 27/12/2016 from:https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2015.pdf

68. Danielle Correa, "Malaysian police works with Interpol and FBI to evade cyber-warfare threat", SC Magazine UK, August 19, 2015, Retrieved on 27/12/2016 from: https://www.scmagazineuk.com/malaysian-police-works-with-interpol-and-fbi-to-evade-cyber-warfare-threat/article/534554/

69. Avant, Kumar. *"Malaysia's cyber warfare training targets 10,000 security professionals by 2020"***,** MIS Asia, Retrieved on 27/12/2016 from: http://www.mis-asia.com/tech/security/malaysias-cyber-warfare-training-targets-10000-security-professionals-by-2020/

70. Asia-Pacific Economic Cooperation(APEC), *"Cyber Security Awareness Raising Workshop Report"* 2009, p4.

71. CyberSecurity Malaysia,"Natioanal Cyber Security Awareness Master Plan Workshop"
CyberNEWS, Issue 8, Quarter 1, (2015), Retrieved on 27/12/2016 from: http://www.cybersecurity.my/cybernews/2015/Q1/eng/jan.html