الامن السيبراني دراسة في الأهمية والابعاد والتأثير والتحديات

الباحث: سمير عبد الكريم جاسم
وزارة الدفاع

أصبح الأمن السيبراني أحد المرتكزات الأساسية في بنية الأمن الوطني والدولي في ظل التحول الرقمي المتسارع الذي يشهده العالم المعاصر. فمع تزايد الاعتماد على الفضاء السيبراني في إدارة شؤون الدولة، وتشغيل البنى التحتية الحيوية، وتسيير الأنشطة الاقتصادية والعسكرية، برزت التهديدات السيبرانية بوصفها أحد أخطر مصادر المخاطر غير التقليدية التي تواجه الدول والمؤسسات. ولم يعد الأمن السيبراني مقتصراً على حماية المعلومات والأنظمة التقنية، بل امتد ليشمل حماية السيادة الوطنية، واستقرار النظام السياسي، واستمرارية الخدمات الأساسية، والقدرات الدفاعية والعسكرية. وتتجلى أهمية الأمن السيبراني في كونه يشكل بعداً استراتيجياً متكاملاً مع الأبعاد السياسية والاقتصادية والعسكرية، حيث بات الفضاء السيبراني ميداناً جديداً للصراع والتنافس بين الدول، وفي هذا السياق، تتعدد أبعاد الأمن السيبراني لتشمل البعد التقني، والتنظيمي، والتشريعي، والبشري والقانوني، فضلاً عن بعده الاستراتيجي المرتبط بالأمن القومي. أن تعزيز الأمن السيبراني يواجه جملة من التحديات المعقدة، من أبرزها التطور السريع للتقنيات، وتنوع الفاعلين التهديديين، وضعف الأطر القانونية، ونقص الكفاءات المتخصصة.

الكلمات المفتاحية:

الامن السيبراني، الفضاء السيبراني، الدفاع السيبراني، ابعاد الامن السيبراني، تحديات الامن السيبراني.

Cybersecurity: A Study of Its Importance، Dimensions، Impacts، and Challenges

Researcher: Samir Abdul Karim Jasim

Ministry of Defense

Abstract:

Cybersecurity has become one of the fundamental pillars of national and international security in light of the rapid digital transformation characterizing the contemporary world. With the growing reliance on cyberspace in managing state affairs، operating critical infrastructure، and conducting economic and military activities، cyber threats have emerged as one of the most serious sources of non-traditional risks facing states and institutions.

Cybersecurity is no longer limited to the protection of information and technical systems; rather، it has expanded to encompass the protection of national sovereignty، political stability، continuity of essential services، and military and defense capabilities. The importance of cybersecurity lies in its role as a strategic dimension integrated with political، economic، and military dimensions، as cyberspace has become a new arena for conflict and competition among states.

Keywords: Cybersecurity، cyberspace، cyber defense، dimensions of cybersecurity، cybersecurity challenges.

المقدمة:

يعد الأمن السيبراني اليوم أحد الركائز الجوهرية في منظومة الأمن الوطني والدولي، في ظل التحول الرقمي المتسارع الذي أعاد تشكيل طبيعة التهديدات ومصادرها وأدواتها. فقد أدى التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات، والاعتماد المتزايد على الفضاء السيبراني في إدارة شؤون الدولة وتشغيل البنى التحتية الحيوية وتسيير الأنشطة الاقتصادية والعسكرية، إلى بروز تهديدات سيبرانية معقدة تمثل أحد أخطر أنماط المخاطر غير التقليدية التي تواجه الدول والمؤسسات. ولم يعد مفهوم الأمن السيبراني مقتصراً على حماية البيانات والأنظمة التقنية فحسب، بل تطور ليشمل حماية السيادة الوطنية، وضمان الاستقرار السياسي، واستمرارية الخدمات الأساسية، وصون القدرات الدفاعية والعسكرية.

وتنبع أهمية الأمن السيبراني من كونه بعداً استراتيجياً متكاملاً مع الأبعاد السياسية والاقتصادية والعسكرية للأمن القومي، حيث أصبح الفضاء السيبراني ميداناً جديداً للصراع والتنافس والتأثير بين الدول والفاعلين من غير الدول. وفي هذا السياق، تتعدد أبعاد الأمن السيبراني لتشمل الأبعاد التقنية والتنظيمية والتشريعية والبشرية والقانونية، فضلاً عن بعده الاستراتيجي المرتبط مباشرة بالأمن القومي. ومع ذلك، يواجه تعزيز الأمن السيبراني جملة من التحديات المعقدة، أبرزها التسارع التكنولوجي، وتنوع الجهات المهددة، وضعف الأطر القانونية، ونقص الكفاءات المتخصصة، مما يستدعي تبني سياسات واستراتيجيات شاملة قادرة على الاستجابة لطبيعة التهديدات المتغيرة.

أهمية البحث:

تكمن أهمية الأمن السيبراني في دوره الحيوي في حماية السيادة الوطنية وضمان استمرارية عمل مؤسسات الدولة والبنى التحتية الحيوية في ظل الاعتماد المتزايد على الفضاء الرقمي. كما يسهم في تعزيز الاستقرار السياسي والاقتصادي والعسكري من خلال الحد من التهديدات السيبرانية وحماية المعلومات والقدرات الاستراتيجية. ويُعد الأمن السيبراني اليوم بعداً أساسياً من أبعاد الأمن القومي ومجالاً رئيسياً للتنافس والصراع بين الدول.

الإشكالية:

تتمثل إشكالية هذه الدراسة في كيفية قدرة الدول على بناء منظومة أمن سيبراني فعّالة قادرة على مواكبة التحول الرقمي المتسارع، في ظل تصاعد التهديدات السيبرانية وتنوع فاعليها، وتداخل الأبعاد التقنية والتنظيمية والقانونية والاستراتيجية للأمن السيبراني. وتزداد هذه الإشكالية تعقيداً مع محدودية الأطر التشريعية، ونقص الكفاءات المتخصصة، وضعف التنسيق المؤسسي، الأمر الذي يطرح تساؤلات جوهرية حول مدى فاعلية السياسات والاستراتيجيات المعتمدة في حماية الأمن القومي وضمان استمرارية البنى التحتية الحيوية.

الفرضية:

تفترض هذه الدراسة أن تعزيز الأمن السيبراني يعتمد على تبني استراتيجية وطنية شاملة ومتكاملة تجمع بين الأبعاد التقنية والتنظيمية والتشريعية والبشرية، وأن ضعف التنسيق المؤسسي وقصور الأطر القانونية ونقص الكفاءات المتخصصة يؤدي إلى زيادة قابلية الدول للتعرض للتهديدات السيبرانية، بما ينعكس سلباً على الأمن القومي واستقرار مؤسسات الدولة.

أهداف البحث:

١. بيان مفهوم الأمن السيبراني وأهميته في ظل التحول الرقمي المتسارع.

٢. تحليل أبعاد الأمن السيبراني المختلفة، ولا سيما التقنية والتنظيمية، والتشريعية، والبشرية، والاستراتيجية.

٣. توضيح تأثير التهديدات السيبرانية على الأمن القومي واستقرار مؤسسات الدولة والبنى التحتية الحيوية.

٤. تشخيص أبرز التحديات التي تواجه بناء منظومة أمن سيبراني فعّالة.

٥. تسليط الضوء على دور السياسات والاستراتيجيات الوطنية في تعزيز الأمن السيبراني والحد من مخاطره.

هيكلية البحث: تم تقسيم البحث على ثلاث مطالب وكما يلي:

المطلب الاول: مفهوم الامن السيبراني والمفاهيم ذات العلاقة.

المطلب الثاني: ابعاد الامن السيبراني (العسكري، السياسي، القانوني، الاقتصادي، الاجتماعي).

المطلب الثالث: تحديات الامن السيبراني بعد عام ٢٠٠٣

المطلب الاول: مفهوم الامن السيبراني والمفاهيم ذات العلاقة

يعد الأمن السيبراني من أبرز المفاهيم الحديثة في ميدان الأمن الوطني والدولي، إذ ارتبط ظهوره بالنمو المتسارع للتكنولوجيا الرقمية وتوسع استخدام شبكات المعلومات والاتصالات. ومع تعاظم دور الفضاء السيبراني في المجالات الاقتصادية والسياسية والعسكرية، برزت الحاجة إلى وضع إطار مفاهيمي واضح يحدد طبيعة الأمن السيبراني ومضامينه، ويكشف عن علاقته بالمفاهيم الأخرى مثل أمن المعلومات، وأمن الشبكات، والأمن الوطني. إن فهم هذه المفاهيم المتداخلة يُسهم في إدراك الأبعاد الشمولية للأمن السيبراني، ويوضح موقعه في حماية الدول والمؤسسات من التهديدات الرقمية المتزايدة.

أولا: مفهوم الأمن السيبراني

يواجه النظام العالمي اليوم أكبر التحديات الخطرة، فالتقدم التكنولوجي وظهور ثورة المعلومات الرقمية قادت العالم إلى مرحلة تنذر بهيمنة سيبرانية محددة لملامح حروب القرن المستقبلية القادمة فالسيبرانية باختلاف مسمياتها من حرب أو هجمة أو حتى إرهاب غيرت من مفهوم الحرب وشكلها وباتت أهم أداة الحروب الحديثة، لقد دفعت التكنولوجيا للتغيير في كل جوانب الحرب وأركانها ونظرياتها، فحرب الإنترنت أو الحرب السيبرانية تسيطر على النظام العالمي اليوم من ناحية القيادة وهيمنة المعلومات أو حتى المخابرات الرقمية، حيث يشكل هذا المفهوم اليوم مصدر قلق للكثير من الدول لسرعة القدرة الهجومية.

هناك عدد كبير من التعريفات لمصطلح الأمن، ولكن أغلبها تؤكد على انه مجموعة من التدابير والقوانين التي يتبعها الانسان لتحقيق الحماية لنفسه وماله وممتلكاته أو عرضه او اي شيء ثمين يخاف عليه، كما يعرف الأمن باختصار بأنه العمل على التحرر من التهديد، ويعرّف الأمن على مستوى الدول أنه القدرة على حفاظ هذه الدول على كيانها المستقل وتماسكها الاجتماعي والاقتصادي وقوتها العسكرية ضد القوى المعادية من الداخل والخارج.

إن كلمة (cyber) لغة تم استخدامها من قبل عالم الرياضيات نوربرت وينير Novrbert Twiener، حيث كان هو أول من استخدم مصطلح (cyber) عام ١٩٤٨ في أثناء دراسته لموضوع السيطرة والاتصال والقيادة في عالم الحيوان، فضلا عن استخدامه المصطلح نفسه في حقل الهندسة الميكانيكية، ويعود مصطلح (cyber) إلى اللغة اليونانية، والمقصود به علم التحكم الآلي والمستمد من(kubernet Greeks) اليونانية، التي تشير إلى الطيار أو التوجيه[١].

ويشير قاموس (المورد) إلى أنّ السيبرانية هي علم الضبط، وتعود إلى المصدر (cybernetics)، ويُقصد بها هنا ضبط الأشياء عن بعد والتحكم بها والسيطرة عليها

[٢]. وعرّفها قاموس المصطلحات الأمريكية بأنها: فعل يتم عن طريق استخدام الشبكات الإلكترونية بهدف تعطيل أو السيطرة على برامج إلكترونية أخرى. أما تعريف (cyber) اصطلاحاً، فبعضهم صنفها بـ (cyber space) فضاء إلكتروني، وآخرون بـ (cyber War)حرب سيبرانية، وبعضهم (cyber Attacks) هجمات سيبرانية.

لقد ورد مصطلح الأمن السيبراني في العديد من الأدبيات الاكاديمية والحكومية والاعلامية وحتى الشعبية ولكن بوجهات نظر متفاوتة ومتباينة، إن عدم وجود تعريف مقبول على نطاق واسع يستوعب تعدد أبعاد الأمن قد يؤدي الى عرقلة التقدم التكنولوجي والعلمي بسبب تعزيز النظرة التقنية لمصطلح الأمن السيبراني مع فصل باقي التخصصات التي يجب أن تتظافر لمعالجة تحديات الأمن السيبراني المتزايدة التي أصبحت تشمل التحديات السياسية والاجتماعية والاقتصادية فضلاً عن الأطر التنظيمية و القانونية المحلية و الإقليمية والدول التي تمتد عبر الفضاء السيبراني[٣].

وفيما يلي مجموعة من التعريفات الخاصة بمفهوم الأمن السيبراني يمكن أن تغطي أغلب ابعاد هذا المفهوم مع التركيز على الأمني الذي هو مدار اهتمام البحث:

١. تعريف الاتحاد الدولي للاتصالات[*]: الأمن السيبراني هو مجموعة من الادوات والسياسات ومفاهيم الامان والضمانات الأمنية ونهج ادارة المخاطر والاجراءات والتدريب، وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدمين والمالكين[٤].

٢. تعريف جامعة اكسفورد: الأمن السيبراني هو حالة الحماية من الاستخدام الجنائي او غير المصرح به للبيانات الالكترونية، او التدابير المتخذة لتحقيق ذلك.

٣. تعريف السلامة العامة الكندية CNNSI : الأمن السيبراني هو مجموعة من التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة

الحاسوب والبرامج والبيانات من الهجوم او التلف او الوصول غير مصرح به لضمان السرية والنزاهة والتوافر [٥].

٤. تعريف المبادرة الوطنية لدراسات الأمن السيبراني في وزارة الأمن الداخلي الامريكي (DHS): الأمن السيبراني هو النشاط او العملية او القدرة التي تحمي بموجبها انظمة المعلومات والاتصالات والمعلومات الواردة فيها، او يتم الدفاع عنها ضد التلف او الاستخدام غير المصرح به او التعديل او الاستغلال [٦].

بعد استخلاص مجموعة من التعريفات التي تخص الأمن السيبراني يعرّف الباحث الأمن السيبراني بأنه حزمة من الإجراءات الفنية والسياسات لحماية البرمجيات وأجهزة الحاسوب والشبكات، وهو مجموعة من الخطوات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار، ظهر قبل انتهاء الحرب الباردة عام ١٩٨٣ وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وأصبح وسيلة أمنية وحربية دولية أساسية.

ثانيا : الفضاء السيبراني

الفضاء السيبراني هو الوسط التقني الذي تعمل فيه شبكات هائلة من الادوات والوسائل الالكترونية بمكوناتها المختلفة، كأجهزة الكومبيوتر وانظمة الشبكات والبرمجيات وحوسبة المعلومات ونقلها وتخزينها، فهو المجال الرقمي الممتد دولياً عبر خطوط الاتصالات الضوئية والمعدنية والالياف البصرية وموجات الاقمار الصناعية وقنواتها المتعددة في بث خدمة الانترنت والموجات الاخرى [٧].

وعند الرجوع إلى مصطلح الفضاء الإلكتروني (cyber space) فإنَّ هذا المصطلح بدأ بالظهور في عام ١٩٨٤ حينما نشر الروائي الأمريكي ويليام جيبسون[*] William Gibson كتابه الذي يتحدث فيه عن الخيال العلمي في رواية مستحضر الأرواح (Necromancer)، فقد وصف الروائي شبكات كومبيوتر خيالية تحتوي على كم هائل

من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، وأرسى المفاهيم الأساسية للنمو السريع للبيئة الافتراضية.

الفضاء الإلكتروني بوصفه مجالاً افتراضيا ونظام يربط بين عدد من النظم المادية مثلاً موقع (facebook) يستمر بالنمو ويربط أكثر من ملايين الأشخاص بوقت واحد فالمجال السيبراني جعل العالم متشابكا لكنه مفتوح ونطاقه واسع، كما يمتاز الفضاء الإلكتروني بالبصمة الرقمية التي يتركها هذا العالم، فبإمكان أي مستخدم ترك علامة رقمية يمكن استرجاعها ونقلها بسهولة من الآخرين.

وبازدياد التقدم التكنولوجي تحققت قفزات سريعة في مجال الحوسبة وتكنولوجيا المعلومات، ودخلت التكنولوجيا الرقمية في كل مجالات الحياة والبنى التحتية للدول المتقدمة ولاسيما في مجالات الطاقة والمياه والمواصلات والاتصالات والاقتصاد فضلا عن الجوانب العسكرية، فالفضاء السيبراني يمثل الشبكة العالمية لتكنولوجيا المعلومات المترابطة عن طريق الاجهزة والبرامجيات والمعلومات، ويتكون الفضاء السيبراني من ثلاث طبقات[٨]:

أ. الطبقة الاولى: وهي الطبقة المادية التي تتكون من الكهرباء والطاقة والدوائر المتكاملة التي تمثل البنية التحتية للاتصالات واجهزة الارسال والاستقبال.

ب. الطبقة الثانية: تمثل برامج الكومبيوتر التي يتم عن طريقها معالجة المعلومات.

ج. الطبقة الثالثة: هي الطبقة الأخيرة وتكون غير ملموسة حيث تمثل البيانات والمعلومات[*] في عالم العولمة والاتصالات.

يتوقع ان يكون الفضاء السيبراني ساحة جديدة للصراع والحروب السيبرانية التي أخذت في النمو والاتساع، وأخذت الدول الحيطة والحذر من التهديدات السيبرانية وشن الحروب السيبرانية وبشكل مفاجئ يوقف الحياة ويسيطر على كل شيء، وقامت الدول والمؤسسات الأمنية والعسكرية والمدنية في حماية الفضاء السيبراني من خلال الأمن السيبراني، ومن

هنا نشأ شكل من اشكال حماية الفضاء السيبراني من هذه التهديدات ومنها الحروب السيبرانية [٩].

اصبح الفضاء السيبراني الملاذ الذي يتم فيه ومن خلاله العمليات الرقمية كافة للدول والمؤسسات والأفراد ان هذا الاعتماد المستمر ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي شبكة وأمن المعلومات والاتصالات في المجتمع المعلوماتي وأعضائه، إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً في سلامة البنى التحتية للمعلومات الوطنية فكان لابد من ايجاد آلية وقائية وتنظيمية وتشاركية للمحافظة وحماية جميع الأطراف من اي استخدام خاطئ او تهديدات محتملة وهذا يتطلب توفير مظلة امنية لحماية الفضاء السيبراني من خلال مفهوم الأمن السيبراني الذي يختلف عن أمن المعلومات[١٠]. فأمن المعلومات مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها، في حين ان الأمن السيبراني يمثل مجموع الوسائل التقنية والتنظيمية والادارية التي يتم اعتمادها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية الافراد والمؤسسات من المخاطر في الفضاء السيبراني[١١].

ثالثا: الدفاع السيبراني

يقصد بالدفاع السيبراني "مجموعة القدرات النظامية التي تمتلكها القوات العسكرية للحماية من تأثيرات الهجمات السيبرانية والتخفيف من حدتها والتعافي منها بسرعة"، وقد عرفت العقيدة العسكرية الفرنسية الدفاع السيبراني على أنه: "مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن أنظمة المعلومات الحرجة في الفضاء السيبراني"، ووفق الاستراتيجية النمساوية يشير مصطلح الدفاع السيبراني إلى "جميع التدابير اللازمة للدفاع

في الفضاء السيبراني بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية"، كما يعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية والتعامل معها، وتستهدف البنية التحتية لنظم الاتصالات والقيادة والسيطرة"، وفي الاستراتيجية العسكرية البلجيكية يعرف أيضا على أنه "تطبيق تدابير وقائية فعالة للحصول على مستوى مناسب من الأمن السيبراني، وتقليل المخاطر الأمنية إلى مستوى مقبول"(١٢).

وباستثناء التعريف الأخير فإن جميع التعريفات السابقة تطرقت إلى الدفاع السيبراني بمفهومه السلبي، والذي يعني القدرة على استقبال الهجمات السيبرانية وتلافي آثارها سريعا من دون الإضرار بالبنية التحتية والأهداف الاستراتيجية للدولة، أما التعريف البلجيكي فقد أضاف بعدا جديدا وهو الدفاع الإلكتروني الوقائي أو الإيجابي، والذي يعني منع الهجمة قبل حدوثها سواء من خلال اتخاذ تدابير وقائية أو هجمات سيبرانية استباقية، ومن مجمل التعريفات السابقة يمكن تعريف الدفاع السيبراني بأنه " وسيلة لتحقيق الأمن السيبراني من خلال استخدام آليات رصد الهجمات الإلكترونية وتحليلها وتحديد مصدرها، والتخفيف من حدة آثارها على نظم الاتصالات والشبكات والبنية التحتية، وذلك في وقتها الحقيقي مع توافر القدرات الهجومية لتعقب الكيانات وتدمير الشبكات التي انطلق منها التهديد".

كما عرفت الوكالة الوطنية الفرنسية لأمن نظم المعلومات الدفاع السيبراني بأنه: "جميع التدابير التقنية وغير التقنية التي تمكن الدولة من الدفاع في الفضاء الإلكتروني عن أنظمة المعلومات التي تعتبر ضرورية"، وفي الاستراتيجية النمساوية يشير مصطلح الدفاع السيبراني إلى أنه يعني: "جميع التدابير اللازمة للدفاع عن الفضاء السيبراني بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية "٣.

وقد عرفت استراتيجية الأمن القومي الأمريكية لعام ٢٠١٠ الدفاع السيبراني على أنه يعني "تلك الاجراءات التي تجمع بين ضمان المعلومات، والدفاع عن شبكة الحاسوب لتشمل إجراءات الاستجابة)، وحماية البنية التحتية الحيوية مع إمكانات التمكين (مثل دعم البنية التحتية الحيوية للحماية الإلكترونية، وغيرها) لمنع، واكتشاف، والاستجابة في نهاية المطاف لقدرة الخصوم على رفض أو التلاعب بالمعلومات و/ أو البنية التحتية حيث تم دمج الدفاع السيبراني مع الجوانب الدفاعية الديناميكية للحرب السيبرانية لتوفير دفاع في العمق".(١٣)

يشتمل الدفاع السيبراني على ثلاث فئات متكاملة من الأساليب والتي يمكن من خلالها إعاقة الخصم من تنفيذ هجوم سيبراني، والتي يمكن توضيحها فيما يلي (١٤):

١. الدفاع السيبراني الاستباقي : وهي الأنشطة التي تحمي البيئة السيبرانية، وتحافظ على أعلى كفاءة للبنية التحتية السيبرانية والوظائف المهمة من خلال الابتكار لتعزيز الفعل السريع أسرع من المنافسين الاستراتيجيين، وحماية الشبكات والأنظمة والوظائف والبيانات ومواكبة التهديدات والتكنولوجيا السريعة التطور في الفضاء السيبراني، والحفاظ على السلام والأمن السيبراني من خلال تعزيز قدرة الدول بالتنسيق مع الحلفاء على ردع ومعاقبة أولئك الذين يستخدمون أدوات الفضاء السيبراني لأغراض ضارة وذلك من خلال استخدام ونشر الديدان البيضاء (White Worms) وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمة سيبرانية محتملة، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمة نفسها وليس التصدي لها فحسب، كما يشمل أيضا مهاجمة الخصم، وما إن يتم تحديد هوية ومصدر الهجمة، حتى يتم إطلاق هجمة سيبرانية مضادة.

٢. الدفاع السيبراني النشط : يوقف أو يحد من أضرار النشاط السيبراني للخصم، كما يقوم على ردع الأنشطة السيبرانية الضارة، باستخدام جميع أدوات القوة الوطنية لردع الأعداء

عن القيام بأي نشاط في الفضاء السيبراني، الذي يهدد المصالح الوطنية، وإعطاء الإدارة الأولوية لتأمين معلومات وزارة الدفاع، حيث يجب على الدولة حماية شبكاتها من خلال هيئاتها التشريعية، والتأكد من سد أي ثغرات قائمة في قانون الأنترنت.

٣. الدفاع السيبراني التفاعلي: يعمل على استعادة الفعالية، أو الكفاءة بعد الهجوم السيبراني الناجح، هذه الفئات تشكل سلسلة متصلة من أنشطة الأمن السيبراني التي تحدث بشكل مستمر وفي وقت واحد على الشبكات، ووضع سياسات الأمن المعلومات ومراجعتها بشكل دوري.

المطلب الثاني : ابعاد الامن السيبراني (العسكري، السياسي، القانوني، الاقتصادي، الاجتماعي)

نتيجة الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت في العصر الحديث من قبل الحكومات والشركات والمؤسسات والأفراد، ولاسيما القطاعات الحيوية مثل القطاع المالي وقطاعات الطاقة لتقديم خدمات فعالة وعالية الجودة والكفاءة، وما يحمله الفضاء الإلكتروني في طياته من فرص وإمكانيات التوسع في المستقبل، وبسبب طبيعة الفضاء الإلكتروني – غير المقيدة بأي حدود – فقد اتاحت لبعض الجهات المغرضة فرصًا لاختراق بيانات الأفراد والشركات وإلحاق الضرر بهم، لذلك أصبح الحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية أحد أكبر التحديات العالمية التي تواجه جميع الدول [١٥].

تتداخل أبعاد الامن السيبرانية مع الجوانب الاقتصادية والاجتماعية والسياسية والإنسانية انطلاقا من قدرة الدولة على حماية مصالحها وشعبها في مختلف مجالات حياته اليومية ومنها حماية مصادر الثروة في العصر الحالي ونعني بها البيانات والمعلومات والقدرة على الاتصال والتواصل وهي المحور الذي يدور حوله الإنتاج والإبداع والقدرة على المنافسة.

اولا: اهمية الامن السيبراني

تظهر أهمية الأمن السيبراني في الحاجة الملحة للحفاظ على أمان المعلومات والبيانات والأجهزة، ففي العصر الحالي يقوم الأشخاص بتخزين كميات هائلة من البيانات على أجهزة الكمبيوتر والخوادم والأجهزة الأخرى المتصلة والكثير من هذه المعلومات حساسة، مثل معلومات التعريف الشخصية بما في ذلك كلمات المرور أو البيانات المالية، وإذا تمكن أحد المجرمين الإلكترونيين من الوصول إلى هذه البيانات، فيمكن أن يتسبب في حدوث فوضى، عن طريق الاستيلاء على معلومات حساسة، أو استخدام كلمات المرور لسرقة الأموال، أو حتى تغيير البيانات بحيث يستفيد منها المهاجم [١٦].

يعد الأمن السيبراني مهما لأن المؤسسات الحكومية والعسكرية والشركات والمالية والطبية تقوم بجمع ومعالجة وتخزين كميات غير مسبوقة من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى، ويمكن أن يكون جزء كبير من هذه البيانات معلومات حساسة، سواء كانت ملكية فكرية أو بيانات مالية أو معلومات شخصية أو أنواع أخرى من البيانات التي يمكن أن يؤدي الوصول إليها أو التعرض لها بشكل غير مصرح به إلى عواقب سلبية وتقوم المؤسسات بنقل البيانات الحساسة عبر الشبكات والأجهزة الأخرى أثناء ممارسة الأعمال التجارية، ويصف الأمن السيبراني الانضباط المخصص لحماية تلك المعلومات والأنظمة المستخدمة لمعالجتها أو تخزينها [١٧].

إنَّ اغراض ابحاث واستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية أو الأدائية وكذلك هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها [١٨]:

١. السرية أو الموثوقية. وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك.

٢. التكاملية وسلامة المحتوى. التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

٣. استمرارية توافر المعلومات او الخدمة. التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها.

٤. عدم إنكار التصرف المرتبط بالمعلومات ممن قام به. ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين.

مع تزايد حجم الهجمات السيبرانية وتعقيدها، فإن الشركات والمنظمات، وخاصة تلك المكلفة بحماية المعلومات المتعلقة بالأمن القومي، الصحية أو المالية، بحاجة إلى اتخاذ خطوات لحماية المعلومات الحساسة المتعلقة بأعمالهم وموظفيهم، وفي وقت مبكر من مارس ٢٠١٣، حذر كبار مسؤولي الاستخبارات في البلاد من أن الهجمات السيبرانية والتجسس الرقمي هي أكبر تهديد للأمن القومي، متفوقة حتى على الإرهاب وحتى يتحقق الهدف من الحماية السيبرانية لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك ومن أهمها ما يلي[١٩]:

١. التقنية. تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

٢. الأشخاص. يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.

٣. الأنشطة والعمليات. يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

ثانيا: الأبعاد العسكرية للأمن السيبراني

تنشأ اهمية الامن السيبرانية في هذا البُعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي الى نشأة الحروب والصراعات المسلحة، والاختراقات التي تؤدي الى نشأة الحروب والصراعات المسلحة، واختراقات انظمة المنشآت النووية وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي الى كوارث [٢٠].

كما يشمل هذا البعد الفائق الأهمية على المحافظة على الشبكات العسكرية بين مختلف الوحدات العسكرية مما يضمن تبادل آمن للمعلومات العسكرية ويضمن كذلك عدم تعرضها للاختراق من طرف قراصنة الأنترنت، والتي قد تدمر قاعدة البيانات العسكرية الهامة والسرية، مما يعرض الأمن القومي للدول للخطر الكبيرة، وتجدر الإشارة إلى أن بدايات الأنترنت كانت في بيئة عسكرية بشكل أساسي لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والإنجازات العلمية التي تسهم في تفوق بلد على آخر، وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء السيبراني، ومن ثمة تحقيق الأهداف عن بعد، ومن ثم فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد من أي اختراق خارجي سيؤدي بالضرورة إلى شن

هجمات سيبرانية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات وما يلحقه من مخاطر.

تتراكم الأمثلة التي يمكن سوقها في هذا المجال لتوضيح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية، ومن ابرز النماذج الهجمات السيبرانية التي شنتها الصين على الولايات المتحدة الأمريكية في عام ٢٠٠١م حيث تعرض ما يقارب من (١٢٠٠) موقع امريكي لهجمات من قراصنة صينيين في الفترة من ٣٠نيسان وحتى ٧ أيار عام ٢٠٠١م، وقد شملت الهجمات مواقع البيت الابيض والقوات الجوية الامريكية ووزارة الطاقة الامريكية، كما قام قراصنة صينيون بشن بضع هجمات على شركة (لوكهيد مارتن) الأمريكية المختصة بصناعة الأسلحة إذ سرقوا معلومات عن تكنولوجيا تصنيع مقاتلة (إف – ٣٥) التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة (جي – ٢٠) الصينية، كما شملت الهجمات السيبرانية أيضا مقاولين لدى وزارة الدفاع الامريكية يعملون على صناعة وتطوير الطائرات بدون طيار الامريكية بهدف سرقة معلومات حول هذه الطائرة[٢١].

حدثت عدة اختراقات لأنظمة المنشآت النووية في إيران وتبين امكانية الاختراق والتلاعب بها مع ما يعنيه ذلك من تهديد للأمن القومي للدولة المعنية ومن تعريض السلام الدولي للاهتزاز في هذا المجال ايضا، يمكن ايضا ايراد الاختراق الذي حصل في البرازيل والمملكة المتحدة للبنية التحتية للطاقة حيث انقطع التيار الكهربائي ما طال آثاره السلبية ملايين الاشخاص والمؤسسات والمصالح[٢٢].

وجه خبراء اميركيون خطاباً مفتوحاً الى الرئيس الامريكي الاسبق جورج بوش الابن في ايلول عام ٢٠٠٧ محذرين اياه من خطر الهجمات السيبرانية على البنية التحتية الامريكية التي تضم فضلاً عن الدفاع إمدادات الطاقة الكهربائية والمياه والاتصالات السلكية واللاسلكية والخدمات الصحية والنقل والانترنت في هجمات سيبرانية تشبه

السيناريو الافتراضي (بيرل هاربر) يبقى السيناريو الذي تخيله حمدون توريه حول النتائج الكارثية في عام ٢٠١١، حيث وصف النتائج الكارثية نتيجة الهجمات التي ستأتي دون مقدمات وتعم الفوضى وتنهار جميع الخدمات التجارية، الجوية، والصحية، العسكرية، والحكومية، التي يمكن ان تتجسد فيها المخاطر هي افضل ما يمكن ان يعبر عن جدية الامر والحاجة الى العمل لتحقيق هذا الامن لا سيما وان كلفة التقاعس وانتظار وقوع الكارثة يجعلان نتائجها اكثر دراماتيكية [٢٣].

أقرت الولايات المتحدة استراتيجية جديدة للأمن السيبراني في عام ٢٠١٨م تتضمن موقفا أكثر صرامة في الحرب السيبرانية، وذلك مقابل تهديدات كل من الصين وروسيا وآخرين، ودخلت حيز التنفيذ بعد قرار الرئيس الأمريكي دونالد ترامب بإلغاء قواعد حددها سلفه باراك اوباما للعمليات السيبرانية والاتجاه للاستعداد للحرب السيبرانية من خلال بناء قوة أكثر فتكا وتوسيع التحالفات والشراكات وان قيام أي دولة بنشاط سيبراني ضدها سيكون الرد بطريقة هجومية ودفاعية ولن يتم بالضرورة في الفضاء السيبراني فقط.

ان فشل عملية ردع الانشطة السيبرانية التي تشكل استخداما للقوة ضد الولايات المتحدة الامريكية او حلفائها ستدفع الى استخدام القوة المشتركة من القدرات العسكرية ردا على ذلك في الاتجاه المادي والاتجاه كذلك الى تبني استراتيجية قائمة على (الهجوم الدفاعي) والتحرك الى الامام خارج الحدود واختراق شبكات الخصم وتعزيز القدرات لجمع المعلومات الاستخبارية والاستعداد للصراعات المستقبلية[٢٤].

ثالثا: الابعاد الاجتماعية للأمن السيبراني

تسمح طبيعة شبكة الانترنت المفتوحة عبر المدونات وشبكات التواصل الاجتماعي للمواطن أن يعبّر عن تطلعاته السياسية وطموحاته الاجتماعية بأشكالها كافة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته، وسيلة لإغناء هذا المجتمع وتطويره، بما تتيحه من فرص للاطلاع على الافكار والمعلومات المختلفة، وبما تكوّنه من حاجة لدى

الجميع في الحفاظ على استقرار الفضاء السيبراني والمجتمع الذي يرتكز اليه، والمعلوم أن انفتاح مجتمع ما، على مجتمع آخر، يؤسس لتبادل خبرات وافكار وتكوّن حاجات جديدة وآفاق تعاون وتكامل، وهنا يكمن اهمية الحماية السيبرانية في حماية وصيانة القيم الجوهرية في المجتمع كالانتماء، المعتقدات الدينية والعادات والتقاليد [٢٥].

ان ما تقدمه شبكة الانترنت من امكانات وقدرات للمجالات العلمية والثقافية والخدماتية يمكن ان يضيف الى ما سبق ذكره حيث تسمح بالوصول إلى مناطق بعيدة وإلى فئات محددة ككبار السن والمرضى وغيرهم من ذوي الاحتياجات الخاصة، هذا عدا الدور الذي يمكن أن تؤديه في تبادل المعلومات في أوقات الأزمات الانسانية والكوارث بحيث تتأمن المساعدات، وتوزع بالسرعة المطلوبة. ولا تقف الأبعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية والإفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع كالانتماء والمعتقدات فضلاً عن العادات والتقاليد عبر إنشاء المجموعات التي تهتم بنشر الوعي حول هذه المسائل[٢٦].

يأتي التشديد من قبل المنظمات والهيئات الدولية على نشر ثقافة الأمن في الفضاء السيبراني وضرورة تعاون المجتمع بكل مكوناته على تحقيقه وضمانه، فمما لا شك فيه أن المخاطر السيبرانية تطال المجتمع ككل، سواء بسبب ارتكاز الخدمات الحيوية كالطاقة والنقل والصحة والاتصالات، وغيرها على ما تقدمه تقنيات الاتصالات والمعلومات من امكانات أو عبر ما يضخ من محتوى في الفضاء السيبراني' فالمحتويات غير المشروعة ذات تأثير سلبي أكيد على أخلاقيات مجتمع معين وعلى ارتفاع نسبة الممارسات الجرمية.

الأمثلة التي تساق هنا كثيرة ونذكر منها الترويج للاتجار بالممنوعات، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين، وعليه لا بد من بناء مجتمع مسؤول ومدرك

لمخاطر الفضاء السيبراني، قادر على التعامل بحد أدنى من قواعد السلامة مع إدراك للعواقب القانونية التي يمكن أن تترتب على بعض التصرفات التي تمارس في الفضاء السيبراني[٢٧].

رابعا: الأبعاد السياسية للأمن السيبراني

هناك العديد من القضايا التي تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، حيث تخلق تسريبات الملفات السرية والاختراقات الخطيرة الحواسيب الدول ومنظوماتها الرقمية أزمات سياسية ودبلوماسية، كما أن الفضاء السيبراني أصبح من الآليات المستعملة حديثا في الحملات الانتخابية المختلفة، إذ أدى الدور المتنامي لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية تظاهرات افتراضية، حركات احتجاجية إلكترونية إلى استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها، وحتى المعارضة، وفي سياق آخر يتم استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، واعتمادها آلية للاتصال بينها كأفراد وجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الأنترنت [٢٨].

لذلك تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها، ومصالحها الاقتصادية التي تعنى حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر التقنيات في موازين القوى داخل المجتمع نفسه، إذ أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي في اللعبة السياسية. كما أصبح بإمكانه الاطلاع، على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول اليها ويمكن أن توزع وتنشر على الانترنت وبقية الأجهزة التي توصل بها[٢٩].

يستمر العاملون في الشأن السياسي بالإفادة مما تقدمه هذه التقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين والترويج لسياساتهم في العالم، وغني عن البيان مدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي يروج لها، فقد استخدم اوباما مثلا الشبكات الاجتماعية بشكل كثيف خلال حملته الانتخابية، كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر موقع الويكيليكس أثرا سلبيا على العلاقات بين الدول وعلى مصداقيتها.

خامسا: الأبعاد الاقتصادية للحماية السيبرانية

أصبحت الأنترنت فضاء خصبا لكل تلك المعاملات الاقتصادية في ميدان التجارة والصناعة والاستيراد والتصدير والمعاملات البنكية والمصرفية بين الدول وبين الأفراد تطويرا للاقتصاد الوطني، مما يدعو الى الاهتمام بهذا النوع من الأمن السيبراني في هذا المجال الحيوي الذي يهدف الى تحقيق التنمية للدول المترابطة بشبكة إلكترونية قوية يخشى عليها من الاختراقات التي قد تعطل مسارات تلك التنمية، بل وقد ترهن مستقبل تلك العلاقات الاقتصادية بين الدول والمجتمعات، لذلك أصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين، الأمر الذي جعل من استخدام الكمبيوتر وشبكة الأنترنت في تطوير الصناعات وتحريك الاقتصاد ومعالجة كل المعاملات الاقتصادية والمالية يزيد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

ترتبط حماية الأمن السيبراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تكنولوجيا المعلومات والاتصالات، وبالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كذلك تتيح تكنولوجيا المعلومات والاتصالات تعزيز التنمية الاقتصادية لبلدان كثيرة عبر افادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة

إنتاجها بأفضل الشروط، الا ان هذا الواقع المشرق يطرح مسائل مختلفة سواء منها ما يتعلق بحماية مقدم الخدمة والعمل أو بحماية المستهلك على الانترنت(٣٠).

ان دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الإلكترونية اذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، وبحفظ المال في المحفظة الإلكترونية وبالإيفاء من خلالها، وباستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال، فضلا عن ما يمكن أن يثيره هذا الأمر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطرة والعابرة للحدود كتبييض الأموال والتهرب من الضريبة وانتهاك الامن المعلوماتي (٣١).

يربط المسؤولون عن مقدرات الحكومات وسياساتها بين الأمن والنمو الاقتصادي بشكل واضح فالأمن السيبراني يضمن ركون الجمهور إلى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس اقتصاد سليم ولعل الدليل الأوضح على هذه القيمة هو استهداف هذه المعلومات، منذ القديم سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الاعتداء على الملكية الفكرية. هذا عدا التأثيرات المالية السلبية التي يتركها الاعتداء على أنظمة المعلومات وتعطيلها كما في سرقة نتائج أبحاث أو غيرها من معلومات أو كتفشي الفيروسات على غرار ما حصل مع فيروس الحب(*) والذي انطلق من الفلبين، في العام ٢٠٠٠.

سادسا: الأبعاد القانونية للأمن السيبراني

يرتب النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني نتائج قانونية وموجبات تستدعي اهتماما خاصا لجهة إيجاد القواعد الخاصة بحل النزاعات التي يمكن أن تنشأ عنها لذا لا بد من مراعاة بعض التحولات التي رافقت ظهور مجتمع المعلومات، فيما

يخص الحقوق الأساسية والحريات الإنسانية المعترف بها في الدساتير والتشريعات الدولية، أضيفت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية والحق في إنشاء التجمعات على الانترنت، كما الحق في حماية ملكية البرامج المعلوماتية.

ظهرت كلف اقتصادية ومنها على سبيل المثال عملية الاحتفاظ ببيانات الاتصالات لغرض التحقيق الجنائي في المخالفات والجرائم الخاصة بالمحتوى، وما يعنيه هذا الامر من كلفة خاصة بحفظ المحتوى وإدارته، ويبقى أن المحور الأساس في حماية الأشخاص والمؤسسات على السواء حماية البيانات لاسيما الشخصية والحساسة منها فضلاً عن حماية الحق في الخصوصية، وذلك يضاف إلى ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية والتجارية في ضوء الحاجة إلى إعادة صياغتها بما ينسجم مع توسع استخدام الشبكات الاجتماعية والمسائل القانونية التي لا بد أن تثار، على مستوى حماية المستهلك والخصوصية والبيانات الشخصية وحقوق العمال والمستخدمين والملكية الفكرية، فالسنوات القادمة لا بد أن تشهد تصاعدا في أعداد الأعمال الجرمية والممارسات غير القانونية في الفضاء السيبراني ما يعني عمليا ازدياد عدد القضايا التي سترفع امام المحاكم ما يستدعي إعداد البيئة التنظيمية والتشريعية وبناء قدرات هيئات المكافحة والحكم [٣٢].

سابعا: الابعاد التكنولوجية للأمن السيبراني

يتمثل في الارتباط المتزايد بتكنولوجيا الاتصال والمعلومات وتوفير فرص امام لاعبين جدد وبخاصة مع ما وفره الانترنت وكونه وسيلة سهلة ورخيصة وسريعة الانتشار، فضلا عن اندماج الخدمات مع بعضها بحيث تتيح الشبكة خدمة الاتصال وامكانية التراسل المجاني، فضلاً عن الحرية المتاحة وارتفاع سقفها عن وسائل الإعلام التقليدية [٣٣].

إنَّ مجتمع المعلومات أمكن تحقيقه بفعل إدماج تكنولوجيا المعلومات والاتصالات في كل مجال من مجالات النشاط البشري الذي يجعل الأفراد والمنظمات والبلدان متزايدة الاعتماد على البنى التحتية المترابطة شبكياً على النطاق العالمي، وان الدولة التي لا تمتلك التكنولوجيا السيبرانية المحصنة امنيا، سيصبح فضاؤها السيبراني المتضمن للأصول والموارد والمعلومات والخدمات والبنية التحتية التابعة لجميع القطاعات الحيوية (التجارية، الأمنية، العسكرية، المصرفية، الصحية، التعلمية، السياحية، الاقتصادية وغيرها) عرضة للهجمات والتهديدات السيبرانية (الاختراق، القرصنة، التخريب، التلاعب والسرقة) وسيؤدي ذلك الى نتائج كارثية على امنها الوطني.

إنّ مظاهر الحرب السيبرانية قائمة ومستمرة لكن لها طبيعتها الخاصة من حيث الفاعلون فيها، وميدان المعركة، ونوعية الخسائر، وتوقيت المعركة، كما ان هذه الحرب لا تفرق بين المدني والعسكري وهو ما يهدد الأمن الإنساني للأفراد، أما ميدان المعركة فهو بيئة مصنوعة وليست طبيعية تحكمها عوامل الطبيعة ولا يستطيع القانون الدولي ان يحكم التفاعلات التي تجري فيها ليس فقط لغياب مفهوم السيادة فيها ولكن لصعوبة معرفة الفاعل الحقيقي الذي قام بشن هذه الحرب، وقد تكون الأبعاد فيها مباشرة تتمثل في تدمير البيانات، والبنى التحتية، والمعدات العسكرية، وقد تكون الأبعاد غير مباشرة تتمثل في تراجع التنافسية الاقتصادية للدولة، وفقدان الثقة في الاقتصاد الوطني وقد فرض ذلك العديد من التحديات على مفهوم الأمن الوطني بصورته التقليدي.

مما سبق يتبين ان الحماية السيبرانية أصبحت ذات أهمية متزايدة في عالم اليوم، ومع تزايد تخزين البيانات ونقلها إلكترونيًا، زاد أيضا خطر الهجمات السيبرانية، ويتيح الأمن السيبراني حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به، وبالتالي حماية الخصوصية والسرية والملكية الفكرية.

المطلب الثالث : تحديات الامن السيبراني بعد عام ٢٠٠٣

تواجه مؤسسات الأمن السيبراني تحديات استثنائية ناجمة عن التعقيد المتزايد وتكرار التهديدات السيبرانية، إن تكامل التقنيات المتقدمة مثل الذكاء الاصطناعي والحوسبة الكمومية في مجال الأمن السيبراني يجلب آفاقًا واعدة وعقبات هائلة، يعزز الذكاء الاصطناعي قدرات الكشف عن التهديدات والاستجابة لها مع تزويد الخصوم بأدوات لشن هجمات أكثر تعقيدًا، مثل التصيد الاحتيالي المدعوم بالتزييف العميق ومخططات الهندسة الاجتماعية المدعومة بالذكاء الاصطناعي، فضلا عن ذلك فإن ظهور الحوسبة الكمومية يهدد أساليب التشفير التقليدية، مما يستلزم إنشاء أساليب تشفير مقاومة للحوسبة الكمومية على الفور، ويؤكد هذا التأثير المزدوج للتكنولوجيات الناشئة على الحاجة الملحة لقادة الأمن السيبراني للتكيف والابتكار باستمرار.

لقد شهد العام الحالي زيادة ملحوظة في سرعة التخفي والهجمات الإلكترونية، مما يشير إلى تحول كبير في ديناميكيات التهديد. يستخدم الخصوم تكتيكات متقدمة لتجاوز تدابير الأمن التقليدية باستخدام بيانات اعتماد وأدوات شرعية للتهرب من الاكتشاف، ونتيجة لذلك، يجب على قادة الأمن السيبراني تعزيز إشرافهم الاستراتيجي وتنفيذ تدابير أمنية قوية لمعالجة هذه التحديات المتطورة بشكل شامل.

مع تزايد تعقيد المشهد السيبراني، أصبح دور قادة الأمن السيبراني أكثر أهمية من أي وقت مضى، يتعين عليهم مواكبة التقدم التكنولوجي السريع وتنمية ثقافة تنظيمية استباقية ومرنة قادرة على تحمل التهديدات المعقدة في المستقبل، ويظل تحقيق التوازن بين الحفاظ على بروتوكولات أمنية قوية قابلة للتكيف مع دعم الابتكار والإنتاجية التنظيمية يشكل تحديًا محوريًا للقادة في هذا المجال، ومن أبرز تحديات الامن السيبراني العالمية ما يأتي:

اولا: مواكبة التهديدات المتطورة

يتطور الأمن السيبراني بسرعة بسبب التقدم في الذكاء الاصطناعي والحوسبة الكمومية[٣٤]* وقد حسنت هذه التقنيات استراتيجيات الدفاع ومكنت مجرمي الإنترنت من تنفيذ هجمات أكثر تعقيدًا بسرية وكفاءة أكبر. يستخدم مجرمو الإنترنت الذكاء الاصطناعي في أنشطة مثل التصيد الاحتيالي باستخدام تقنية التزييف العميق وتطوير برامج ضارة معقدة يمكنها تجاوز تدابير الأمن التقليدية. وهذا يفرض تحديات جديدة على فرق الأمن السيبراني التي يجب أن تستجيب بشكل ديناميكي واستباقي، ولمكافحة هذه التهديدات بشكل فعال يجب على المنظمات تكامل تقنيات الأمان التكيفية التي تستخدم التعلم الآلي لتحديد وتحييد التهديدات المحتملة قبل حدوثها سيضمن هذا تحديث بروتوكولات الأمان باستمرار لمعالجة أحدث نقاط الضعف [٣٥].

ثانيا: استقطاب الموهوبين الهواة

إن الحاجة إلى خبراء الأمن السيبراني المهرة تتزايد، مما يجعل جذب المواهب والاحتفاظ بها أمرًا صعبًا. ولمعالجة هذا الأمر، تقدم الشركات الكبرى رواتب جذابة وامتيازات واسعة وفرصًا لتحسين المهارات بشكل مستمر. فضلا عن ذلك، فإنها تعطي الأولوية لإنشاء بيئة عمل داعمة تعزز التوازن بين العمل والحياة والنمو المهني. إن ضمان حصول فرق الأمن السيبراني على أحدث الخبرات والقدرات أمر بالغ الأهمية. كما أن الاستثمار المستمر في برامج التدريب والشهادات أمر بالغ الأهمية لإبقائهم على اطلاع دائم على مشهد التهديدات المتطور باستمرار والتقنيات المتطورة.[٣٦]

ثالثا: تحقيق التوازن بين الأمان وسهولة الاستخدام

يواجه مديرو الأمن السيبراني باستمرار تحديًا يتمثل في الموازنة بين تدابير الأمن القوية والحاجة إلى الكفاءة التنظيمية وسهولة الاستخدام، يمكن أن تعيق بروتوكولات الأمن الصارمة للغاية الإنتاجية وتزعج المستخدمين، في حين قد تترك السياسات المتساهلة الأنظمة الحيوية عرضة للهجمات. يكمن الحل في صياغة استراتيجيات أمنية تتكامل

بسلاسة مع سير عمل المستخدم والعمليات التجارية. يعد الفهم الشامل للمشهد التكنولوجي والمتطلبات الخاصة للشركة أمرًا ضروريًا لتنفيذ هذه الاستراتيجية بنجاح وهذا يضمن أن بروتوكولات الأمن يمكنها تعزيز العمليات اليومية من دون التسبب في عوائق.

رابعا: التواصل الفعال

تعتمد فعالية استراتيجيات الأمن السيبراني بشكل كبير على التواصل الواضح بين فرق الأمن السيبراني وأصحاب المصلحة غير الفنيين. يجب أن يكون قادة الأمن السيبراني ماهرين في ترجمة التفاصيل الفنية المعقدة إلى رؤى قابلة للتنفيذ تتوافق مع مختلف الإدارات داخل المنظمة. من الضروري إتقان هذه القدرة على تنفيذ تدابير أمنية ناجحة وتشجيع بيئة مؤسسية تعطي الأولوية للوعي الأمني وتعززه. من خلال تعزيز التواصل، يمكن لقادة الأمن السيبراني ضمان فهم بروتوكولات الأمان والالتزام بها عبر جميع مستويات المنظمة، ومن ثم تعزيز موقف الأمن العام.[٣٧]

خامسا: البقاء ضمن الميزانية

إن إعداد ميزانية الأمن السيبراني يشكل تحديًا استراتيجيًا يتطلب موازنة التكاليف مع ضرورة وجود آليات دفاع قوية. وفي ظل الموارد المحدودة، يتعين على قادة الأمن السيبراني إعطاء الأولوية للاستثمارات في التقنيات والممارسات التي توفر أعلى عائد على الاستثمار في الأمن. وتتضمن العملية عادةً اختيار المخاطر التي يجب الحد منها من خلال النظر في عواقبها المحتملة واحتمالاتها. كما تتطلب إدارة الميزانية الفعّالة مراجعة مستمرة وتعديلًا لمواءمة التهديدات الناشئة والتغييرات التنظيمية، مما يضمن استخدام الموارد المالية بكفاءة للحفاظ على موقف أمني قوي من دون الإفراط في الإنفاق.

سادسا: إدارة الفرق عن بُعد

أدى تزايد العمل عن بعد إلى ظهور صعوبات محددة في إدارة فرق الأمن السيبراني التي غالبًا ما تنتشر عبر مواقع ومناطق زمنية مختلفة. وتتطلب إدارة الفريق عن بعد بشكل فعال أدوات واستراتيجيات اتصال قوية والتركيز القوي على بناء الثقة والتماسك بين أعضاء الفريق وتعد الاجتماعات الافتراضية المنتظمة وقنوات الاتصال الواضحة والمتسقة والوصول إلى أدوات التعاون ضرورية للحفاظ على محاذاة الفريق وإنتاجيته. وعلاوة على ذلك، فإن الاستثمار في برامج التدريب والتطوير في مجال الأمن السيبراني التي يمكن الوصول إليها عن بعد يضمن أن جميع أعضاء الفريق لديهم المهارات اللازمة لمعالجة التهديدات المتطورة، بغض النظر عن الموقع [٣٨].

سابعا: مواكبة متطلبات الامتثال

مع تطور لوائح الأمن السيبراني، فإن الالتزام بها أمر بالغ الأهمية لقادة الأمن السيبراني. ويتطلب ذلك البقاء على اطلاع بأحدث التغييرات التنظيمية وفهم كيفية تأثيرها على العمليات التنظيمية. ويجب على القادة تطوير استراتيجيات لتكامل الامتثال بسلاسة في العمليات اليومية من دون تعطيل وظائف العمل. ويجب إجراء عمليات تدقيق امتثال منتظمة؛ ويجب أن يتلقى الموظفون تدريبًا على معايير الامتثال، ويجب تنفيذ حلول التكنولوجيا التي تعمل على أتمتة إدارة الامتثال. ومن خلال إعطاء الأولوية للامتثال، تتجنب المؤسسات الغرامات والقضايا القانونية وتعزز سمعتها في الموثوقية والثقة في التعامل مع المعلومات الحساسة.

ثامنا: معالجة التهديدات الداخلية

تظل التهديدات الداخلية بالغة الأهمية في مجال الأمن السيبراني، وتشمل الخروقات غير المقصودة والتخريب المتعمد. ينشر قادة الأمن السيبراني الفعالون مجموعة من أدوات المراقبة المتقدمة وضوابط الوصول القوية والتدريب المستمر للموظفين للتخفيف من هذه المخاطر. إن تطبيق مبدأ الحد الأدنى من الامتيازات، الذي يقيد وصول الموظفين إلى

الموارد الأساسية فقط لوظائفهم، يمكن أن يخفف بشكل كبير من المخاطر المرتبطة بالتهديدات الداخلية. تعد عمليات التدقيق المنتظمة وتحليلات السلوك ضرورية لتحديد الأنشطة الشاذة التي قد تشير إلى انتهاك أمني. يعد تثقيف الموظفين حول أفضل ممارسات الأمن السيبراني وكيفية التعرف على علامات التصيد الاحتيالي والهجمات الشائعة الأخرى أمرًا ضروريًا لتعزيز دفاعات المؤسسة. هذا ضروري للحد من التهديدات الداخلية من خلال تعزيز الوعي واليقظة بين أعضاء الفريق.

الخاتمة:

تُظهر هذه الدراسة أن الأمن السيبراني لم يعد خياراً تقنياً أو إجراءً احترازياً محدوداً، بل أصبح مكوّناً استراتيجياً أساسياً من مكونات الأمن القومي في العصر الرقمي. فقد أدى التوسع المتسارع في استخدام الفضاء السيبراني إلى تعقيد بيئة التهديدات، وخلق أنماط جديدة من المخاطر التي تستهدف الدول ومؤسساتها وبناها التحتية الحيوية، بما يتجاوز المفاهيم التقليدية للأمن والدفاع. وبينت الدراسة أن فعالية الأمن السيبراني ترتبط ارتباطاً وثيقاً بمدى تكامل أبعاده التقنية والتنظيمية والتشريعية والبشرية والاستراتيجية، وأن أي خلل في أحد هذه الأبعاد ينعكس سلباً على قدرة الدولة في مواجهة التهديدات السيبرانية.

كما خلص البحث إلى أن التحديات التي تواجه الأمن السيبراني، مثل التطور السريع للتقنيات، وتنوع الفاعلين التهديديين، وضعف الأطر القانونية، ونقص الكفاءات المتخصصة، تفرض على الدول تبني رؤى وسياسات شاملة تتسم بالمرونة والتحديث المستمر. وفي هذا الإطار، يبرز دور الاستراتيجيات الوطنية للأمن السيبراني في تعزيز التنسيق المؤسسي، وبناء القدرات البشرية، وتطوير الأطر القانونية والتنظيمية، بما يسهم في حماية السيادة الوطنية وضمان استمرارية عمل مؤسسات الدولة. وعليه، فإن الاستثمار في الأمن السيبراني يمثل استثماراً مباشراً في استقرار الدولة وأمنها ومستقبلها في بيئة دولية تتسم بتزايد الاعتماد على الفضاء الرقمي وتنامي التهديدات المرتبطة به.

الاستنتاجات:

١. إنَّ الأمن السيبراني يشكّل بعداً استراتيجياً أساسياً من أبعاد الأمن القومي، ولم يعد يقتصر على الجوانب التقنية، بل أصبح مرتبطاً بحماية السيادة الوطنية واستقرار الدولة ومؤسساتها.

٢. تُظهر التهديدات السيبرانية المعاصرة طابعاً معقداً ومتطوراً، نتيجة التسارع التكنولوجي وتعدد الفاعلين التهديديين من دول وجماعات منظمة وأفراد، مما يزيد من صعوبة مواجهتها.

٣. تعتمد فعالية منظومة الأمن السيبراني على مدى تكامل الأبعاد التقنية والتنظيمية والتشريعية والبشرية، وأي خلل في أحد هذه الأبعاد يضعف القدرة على الردع والحماية.

٤. يشكّل ضعف الأطر القانونية ونقص الكفاءات المتخصصة والتنسيق المؤسسي غير الفعّال من أبرز التحديات التي تحد من كفاءة الأمن السيبراني في العديد من الدول.

٥. إن تبني استراتيجية وطنية شاملة للأمن السيبراني، قائمة على بناء القدرات وتحديث السياسات وتعزيز التعاون المؤسسي، يُعد شرطاً أساسياً لمواجهة التهديدات السيبرانية وضمان استمرارية البنى التحتية الحيوية.

التوصيات:

١. تطوير استراتيجية وطنية شاملة للأمن السيبراني ترتكز على دمج الأبعاد التقنية والتنظيمية والتشريعية والبشرية، مع تحديثها بشكل دوري لمواكبة التهديدات المتغيرة.

٢. تعزيز القدرات البشرية والتدريب المتخصص من خلال برامج تعليمية وتدريبية مستمرة لتكوين كوادر قادرة على إدارة ومواجهة التهديدات السيبرانية بكفاءة.

٣. تقوية الأطر القانونية والتنظيمية لتوفير بيئة تشريعية واضحة وفعّالة تدعم مواجهة الجرائم السيبرانية وتعزز المسؤولية والمساءلة.

٤. تفعيل التنسيق المؤسسي والتعاون بين الجهات المختلفة الحكومية والخاصة، لضمان استجابة سريعة وفعّالة لأي هجوم سيبراني وحماية البنى التحتية الحيوية.

٥. الاستثمار في التكنولوجيا والأدوات الحديثة للكشف عن التهديدات السيبرانية ومواجهتها، بما يشمل نظم المراقبة والتحليل والسيطرة على الشبكات، وربطها بالقدرات الدفاعية الوطنية لضمان الردع والتصدي الفعال.

الهوامش

(١) سامي محمد جمال، امن المعلومات السيبرانية، دار العلم والايمان، القاهرة، ٢٠٢٤، ص ١٩.

(٢) منير البعلبكي، قاموس المورد، دار العلم للملايين، بيروت، ط٣، ١٩٧٠، ص٢٤٣.

(3) Dan Craigen،Nadia Diakun and Randy purse،Defining Cyber security ،،http:// timreview.ca / article ،Canada ،2014،pp.13

(*) الاتحاد الدولي للاتصالات: وهي واحدة من الوكالات الخاصة (specialized agencies) التابعة للأمم المتحدة. يقع المركز الرئيسي للاتحاد في جنيف بسويسرا بجانب مقر الأمم المتحدة هناك.

(4) ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva:International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en ،visit in 2/1/2020.

(5) CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: http://www.ncix.gov/publications/policy.

(6) DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1 ،2014: http://niccs.us-cert.gov/glossary#letter_c

(٧) احمد حسين الربيعي، استراتيجيات مواجهة التهديدات غير النمطية "الإرهاب السيبراني انموذجا"، المجلة العلمية لجهاز مكافحة الإرهاب، المجلد (٤)، العدد (٧)، جهاز مكافحة الإرهاب، ٢٠٢٤، ص١٦٧.

(*) ويليام فورد جيبسون (ولد في ١٧ آذار عام ١٩٤٨) هو روائي أمريكي كندي له طابع خيالي تأملي.

(٨) محمد منذر جلال و سرى غضبان غيدان، تكنولوجيا الحروب السيبرانية واستراتيجيات المواجهة الدولية، دار ومكتبة عدنان للنشر، بغداد، ٢٠٢١، ص١٣٩.

(*) تُعرف البيانات "Data" على أنها حقائق أولية عشوائية غير منظمة وهي غير مجدية للبشر، ولجعلها ذات قيمة فإنه يستلزم معالجتها، وذلك من خلال تحويل البيانات إلى معلومات، بينما تُعرف المعلومات "Information" على أنها بيانات منظمة ومعالجة وتقدم في سياق معين وهي مجدية للبشر.

(٩)علاء عبد الرزاق محمد السالمي، المدخل الى الأمن السيبراني، دار الذاكرة للنشر والتوزيع، بغداد، ٢٠٢١، ص١٠٥.

(١٠) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد (٥٧)، جامعة النهرين، ٢٠١٩، ص٩٦.

(١١) محمد جبار الكريزي، الهجمات السيبرانية وخطورتها على الأمن الوطني والخصوصية، كراس النهرين العدد (١٣)، مركز النهرين للدراسات الاستراتيجية، ٢٠١٩،

(١٢) ايهاب خليفة، القوة الالكترونية: كيف يمكن ان تدير الدول شؤونها في عصر الانترنت، القاهرة، العربي للنشر والتوزيع، ٢٠١٨، ص١١٧.

(١٣) استراتيجية الامن القومي الامريكية لعام ٢٠١٠.

(١٤) كسينجر والان فريدمان، الامن الالكتروني والحروب الالكترونية: دليل اساسي لما عليك معرفته في فضاء الجيل الرابع، دبي، دار قنديل للطباعة والنشر والتوزيع، ٢٠١٨، ص٢٨٥.

(١٥) احمد سلمان داود. استراتيجية الامن السيبراني ودورها في تحقيق الامن الوطني العراقي بعد عام ٢٠١٠، رسالة ماجستير في العلوم السياسية، كلية الدفاع الوطني، الدورة (٢٤)، جامعة الدفاع للدراسات العسكرية العليا، ٢٠٢٠.، ص١٥.

(١٦) خالد ممدوح إبراهيم. مصدر سابق، ص٥٣.

(١٧) المصدر نفسه. ص٥٤.

(١٨) سامي محمد جمال الناقة. امن المعلومات السيبرانية، دار العلم والايمان للنشر، مصر، ٢٠٢٤، ص٨.

(١٩) أحمد عبيس نعمة، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٦٠.

(٢٠) محمد عبد الله شاهين. الامن السيبراني ونظم حماية المعلومات، الاسكندرية، المركز الأكاديمي للنشر، ٢٠٢٥، ص١٥.

(٢١) ايهاب خليفة، الحرب السيبرانية مراجعة العقيدة العسكرية استعدادا للمعركة القادمة، مجلة السياسة الدولية، العدد (٢١١)، مركز الاهرام للدراسات الاستراتيجية، القاهرة،٢٠١٨، ص ١٨.

(٢٢) المصدر نفسه. ص١٩.

(٢٣) منى الاشقر جبور. السيبرانية هاجس العصر، السيبرانية هاجس العصر، ط ١، المركز العربي لمبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، ٢٠١٦، ص٢٨.

(٢٤) التقرير الاستراتيجي العربي لعام ٢٠١٨، الصراع على الفضاء السيبراني بين التوجهات الروسية والامريكية، القاهرة، مركز الاهرام للدراسات السياسية والاستراتيجية، ٢٠١٩، ص٢٧-٢٨.

(٢٥) محمد عبد الله شاهين. مصدر سابق، ص١٦.

(٢٦) منى الأشقر جبور، مصدر سابق، ص٢٩.

(٢٧) عبد الصبور عبد القوي علي مصري، الجريمة الالكترونية، القاهرة، دار العلوم للنشر والتوزيع، ٢٠١٤، ص٨٠.

(٢٨) سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني العدد ٢٦٣، ص

(٢٩) احمد عبد العليم، تحولات القوة في النظام الدولي: القوة السيبرانية، مجلة السياسة الدولية، العدد (٢١٧)، مركز الاهرام للدراسات الاستراتيجية، القاهرة، ٢٠١٩، ص٢٥٢.

(٣٠) الشبكة الدولية للأنترنت. الموسوعة السياسية، الأمن السيبراني – Cyber Security، بالساعة ١٨٠٠ في ٢٠٢٤/١٠/٣٠ https://political-encyclopedia.org

(٣١) اوس مجيد العوادي. الامن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، ٢٠١٦، ص٩.

(*) صنعه شاب فلبيني يعمل في مجال الحاسبات في احدى البنوك في الفلبين وقد سبب خسائر مادية كبيرة عبر العالم.

(٣٢) رغدة البهي. السيبرانية عوامل النشأة وانماط التفاعل، مجلة السياسة الدولية، القاهرة، العدد(٢١٨)، ٢٠١٩،ص١٩.

(٣٣) محمود بري. السيبرانية علم القدرة على التواصل والتحكم والسيطرة، سلسلة مصطلحات معاصرة، العدد(٢١)، المركز الإسلامي للدراسات الاستراتيجية، العتبة العباسية المقدسة، بيروت، ٢٠١٩، ص٢٦.

* **الحاسبات الكمومية:** هو جيل متطور من الحاسبات يعتمد في عمله على مبادئ ميكانيكية الكم بدلا من القواعد التقليدية للفيزياء الكلاسيكية وادناه اهم قدرات الحواسيب الكمومية:

١. حل مسائل معقدة بسرعة هائلة.
٢. تسريع الخوارزميات الرياضية.
٣. محاكاة الأنظمة الفيزيائية والكيميائية بدقة عالية.
٤. تشكل الحواسيب الكمومية تهديدا للتشفير التقليدي كونها قادرة على كسر أنظمة التشفير بسرعة فائقة.

(٣٥) روبرت كرين، ابرز ٢٠ تحدي للأمن السيبراني، تمت المعاينة بالساعة ٢١٠٠ بتاريخ ٢٠٢٥/٨/١٠ على الرابط

https://digitaldefynd.com/IQ/top-cybersecurity-leadership-challenges

(36) Department of Defense. Cybersecurity Test and Evaluation Guidebook، Version 1.0،2019،p18.

(37)'Researchers Found a Hacking Tool that Targets Energy Grids on the Dark Web'، Motherboard، July 2016

(38)What Is Cybersecurity Management? https://www.fortinet.com/