الامن السيبراني واثره على الامن الوطني العراقي

م.د. يسرى ستار بيركة

كلية التربية / الجامعة المستنصرية

ybairgha@uomustansiriyah.edu.iq

ملخص البحث :

تعد الدراسات والبحوث المتعلقة بالامن السيبراني والجريمة الاليكترونية من القضايا التي تشغل اهتمام صناع القرار والباحثين في هذا المجال،نظرا لخطورته وتاثيره على سيادة وامن الدولة وفي هذا البحث سنتطرق الى الامن السيبراني العراقي ومدى تاثيره على الامن الوطني العراقي يتناول البحث ثلاثة محاور رئيسة الاول يناقش ما هية الامن الانساني ومؤشراته فضلا عن مفهوم الامن السيبراني واهدافه وانواعه.فضلا عن ترتيب العراق ضمن مؤشر الامن السيبراني العالمي وخصص المحور الثاني لدراسة اثار الامن السيبراني على الامن الوطني العراقي بابعاده المختلفة اما المحور الثالث فيتناول دراسة السبل والامكانات المتاحة للحد من الهجمات السيبرانية. فكانت مشكله البحث هي ماتاثير الامن السيبراني على الامن الوطني العراقي اما فرضية البحث للامن السيبراني الاثر الكبير على الامن الوطني بكافة ابعاده على العراق وسيادته.

وتوصل البحث على مجموعة من الاستنتاجات اهمها ان للامن السيبراني دور فاعل في حماية امن الدولة ومعلوماتها وبالتالي سيادتها.اما اهم المقترحات فتتمثل بالتوعية باهمية الامن السيبراني على مستوى مؤسسات الدولة والافادة من تجارب الدول التي لها باع طويل في هذا المجال .فضلا عن تخصيص الموارد الكافية لتدريب الكوادر المتخصصة.

الكلمات المفتاحية : الامن ، السيبراني ، الامن الوطني ، الجريمة ، الالكترونية .

Cybersecurity and its impact on Iraqi national security

Assist .dr. Yusra Sattar Birka

College of Education / Al-Mustansiriyah University

Abstract:

Studies and research related to cybersecurity and cybercrime are issues that occupy the attention of decision-makers and researchers in this field, due to its seriousness and impact on the sovereignty and security of the state. In this research, we will address Iraqi cybersecurity and the extent of its impact on Iraqi national security. The research covers three main axes. The first discusses the nature of human security and its indicators, as well as the concept of cybersecurity, its goals and types. In addition to Iraq's ranking in the global cybersecurity index. The second axis was devoted to studying the effects of cybersecurity on Iraqi national security in its various

dimensions. As for the third axis, it deals with studying the available means and capabilities to reduce cyber attacks. The research problem was the impact of cybersecurity on Iraqi national security. As for the research hypothesis, cybersecurity has a great impact on national security in all its dimensions on Iraq and its sovereignty. The research reached a set of conclusions, the most important of which is that cyber security plays an effective role in protecting the state's security and information, and thus its sovereignty. The most important proposals are represented in raising awareness of the importance of cyber security at the level of state institutions and benefiting from the experiences of countries that have a long history in this field. In addition to allocating sufficient resources to train specialized cadres.

Keywords: Security, Cyber, National Security, Crime, Electronic.

المقدمة:

بدءا سنتطرق الى أهم المراحل التي انطلقت منها جرائم المعلوماتية التي ابرزت ضرورة التفكيرالجدي بوجود منظومة للأمن المعلوماتي لمعالجة هذه الجرائم والاختراقات بفظهور استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينييات من القرن الماضي، ظهرت المعالجة الآولى لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكل هذا الموضوع تساؤلا فيما إذا كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة جرمية مستجدة، وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية، فبقيت محصورة في إطار السلوك اللا أخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا وابان سبعينيات القرن الماضي بدأ الحديث عنها كظاهرة جديدة[1]. وفي الثمانينيات ظهر نوع جديد من الجرائم السيبرانية ارتبط بعمليات اقتحام نظم الحاسوب عن بعد، ونشر الفيروسات عبر شبكات الكمبيوتر الذي سبب تدمير الملفات والبرامج، حينها شاع اصطلاح) الهاكرز (المعبر عن مقتحمي النظم ، و بقي الحديث دائما عن دوافع هذه الجرائم محصورا الآمن المعلوماتي السيبراني في اختراق أمن المعلومات و إظهار التفوق التقني من قبل مرتكبي هذه الآفعال الذين لن يتعدوا فئة صغار السن العباقرة هي هذا المجال ، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين و تحديد طوائفهم و لاسيما بعد تحول الجريمة من مجرد مغامرة إلى أفعال تستهدف التجسس و الاستيلاء على البيانات الاقتصادية والاجتماعية و السياسية و العسكرية . شهدت فترة التسعينيات تطورا هائلا في مجال الجرائم التقنية وتغيرا ملموسا في نطاقها ومفهومها بفعل ما أحدثته شبكة الآنترنت من تسهيل لعمليات دخول الآنظمة واقتحام شبكات المعلومات حينما أصبحت مواقع الآنترنت التسويقية النشطة أكثر عرضة للهجمات ،والتي ظهرت بسببها أنماط جديدة من الجرائم، مثل تعطيل النظام التقني ومنعه من القيام بعمله المعتاد الذي يتسبب بانقطاع النظام عن الخدمة لساعات، فتنتج عنه خسائر مالية بالملايين، وقد توسعت جرائم نشر الفيروسات عبر شبكة الانترنت نظرا لسهولة الوصول

1 يحي مفرح الزهراني،الابعاد الاستراتيجية والقانونية للحرب السيبرانية السعودية،مجلة البحوث والدراسات ،جامعة نايف للعلوم الامنية ،العدد23، 2017،ص226

إلى ملايين المستخدمين في الوقت نفسه، ليفتح الباب على مصراعيه لمختلف الأفعال غير السوية المتطورة بتطور التقنية، وقد سجلت عبر هذه المراحل مجموعة من القضايا، منها: قضية)موريس الشهيرة(سنة ١٩٨٨ حينما تم نشر فيروس إلكتروني عرف ب:(دودة موريس) عبر آلاف الكمبيوترات بوساطة الأنترنت، وفي عام 1995 شهدت الأجهزة هجوما عرف باسم-IP SPOOFING ، أدى إلى إيقاف عمل أجهزة أصلية وتشغيل أخرى وهمية، لتبرز قضية الجحيم العالمي التي قام بها بها مكتب التحقيقات الفدرالية مكنتها من اختراق موقع البيت الأبيض الأمريكي[1]، ومن ثم تلتها الكثير من الحوادث كحادثة شركة أوميغا، وفيروس مليسا، وغيرها من جرائم المعلوماتية المتعلقة بالأمن السيبراني . أما في مرحلة ما بعد التسعينيات بعد عام ٢٠٠٠ فقد تطورت هذه الجرائم بنحو أوسع، وتم استخدام المعلومات في الأرهاب المنظم من خلال ضرب البنى التحتية للدول سواء أكانت مرافق عامة أم خدمات أم البنى العسكرية والاقتصادية المتمثلة بالبنوك، وغيرها.

اولا :-مشكلة البحث

ما هي ابعاد الامن السبراني على الامن الوطني في العراق

ثانيا :فرضية البحث

للامن السيبراني ابعاد مختلفة لها علاقة بالامن الوطني كالبعد السياسي والاقتصادي والاجتماعي والعسكري.

ثالثا:هدف البحث

يهدف البحث الى تسليط الضوء على موضوع من المواضيع التي ظهرت في الاونة الاخيرة،الا وهو الامن السيبراني والذي يرتبط ارتباطا كبيرا باستقرار البلدان وضمان سيادتها؟

قسم البحث الى ثلاثة محاور هي:

المحور الاول:ماهية الامن الانساني ومؤشراته

المحور الثاني :اثار الامن السيبراني على الامن الوطني العراقي

المحور الثالث :السبل والامكانات المتاحة للحد من الهجمات السيبرانية

- المحور الاول :ماهية الامن الانساني ومؤشراته

ظهر مفهوم الامن الانساني لاول مرة في تقرير الامم المتحدة للتنمية البشرية عام 1994 ،اذ عرفه" بانه تحرير البشر من التهديدات الشاملة واسعة النطاق والتي تمتد لفترات طويلة وتعرض حياتهم للخطر" يعد الامن من الحاجات الاساسية للنفس وبشكل عام يعني الامن :الاطمئنان الناتج عن الثقة والامن من الوقوع في الفقر او الحرمان او الخوف او العنف ،يعنى الامن الانساني بامن الناس والظروف التي تتعلق بكل فرد في المجتمع لتحقيق العدالة الاجتماعية ،وهو بذلك يبتعد كل البعد عن الحلول العسكرية في حل الازمات والمشكلات ،كما انه يركز على

1 سمير بارة،الامن السيبراني في الجزائر السياسات والمؤسسات ،المجلة الجزائرية للامن الانساني،العدد الرابع،2017،ص270

الاهتمام بالتنمية البشرية والعمل على حل المشكلات قبل وقوعها وتفاقمها وبالتالي تفادي حدوث الحروب والصراعات بين افراد المجتمع الواحد او بين الجماعات .وبهذا فان الامن الانساني يشمل اصعدة مختلفة،اذ يشمل العمل على اصلاح مؤسسات الدولة الداخلية اللازمة لتحقيق الامن الشخصي والسياسي والاقتصادي والاجتماعي والثقافي بالشكل الذي يعزز الشعور لدى الافراد بالانتماء لبلدهم وكمحصلة لذلك سيتقدم المجتمع اقتصاديا وسياسيا وحضاريا.ويمتاز الامن الانساني بخصائص متعددة منها:

1- هومفهوم عالمي يشمل كل دول العالم مهما كانت امكاناتها،بسبب التهديدات الخارجية المشتركة التي تتعرض لها جميع الدول دون استثناء كالارهاب والمخدرات ،وعليه فان اي مساس بالامن الانساني في اي منطقة يستوجب تدخل كل الدول لايقافه وضمان عدم تكراره.
2- الاهتمام بالافراد وامنهم وبالظروف المتعلقة بكل فرد على حدة لتحقيق مبدا العدالة الاجتماعية ،فكما ذكرنا انفا انه يتجنب الحلول العسكرية لحل المشكلات ويهتمبالافراد والتنمية البشرية.
3- من خلال ما سبق يمكن ان نستنتج بان اهم مبدا للامن الانساني هو الاستباق اي حل الازمات والصراعات قبل ان تقع وتتفاقم

-مجالات الامن الانساني: يشمل الامن الانساني مجالات متعددة :

1- الامن الغذائي: تم استخدام هذا المصطلح لاول مرة عام 1970 بسبب انتشار المجاعات حول العالم وهو وضع يتحقق عندما يتمكن الافراد ماديا واقتصاديا وفي جميع الاوقات من الحصول على الغذاء الكافي والسليم والملبي لافضلياتهم الغذائية من اجل حياة صحية ونشطة. وللامن الغذائي اربعة ابعاد رئيسة لكي يتحقق هي:

أ-توفر الغذاء،اي توفر كميات كافية من الغذاء ذو جودة مناسبة عن طريق الانتاج المحلي او عن طريق الاستيراد

ب-امكانية الحصول على الغذاء ،اي تمتع الافراد والاسر بدخل يمكنها من الحصول على الغذاء المناسب عالي الجودة

ج-استغلال الغذاء الذي يتناوله الفرد والتركيز على نوعيته وليس فقط كميته.

د-استقرار الغذاء ،اذ يعد تقلب الاسعار للسلع الغذائية الاساسية وفقدان الاستقرار السياسي والبطالة من اهم العوامل التي تحجم الامن الغذائي.

2- الامن الصحي وهو احد مكونات الامن الانساني هدفه السعي الى تحرير الانسان من التهديدات التي من شانها ان تؤثر سلبا في سلامته الجسدية ،ويشمل انشطة واجراءات عبر الحدود الدولية تخفف من حوادث الصحة العامةلتامين صحة السكان ،كما ويشمل الانشطة المطلوبة لتقليل خطر حوادث الصحة العامة الحادة وتخفيف تاثيرها الذي يعرض سكان منطقة ما الى الخطر،ويرى انصار الامن الصحي انه على جميع الدول ان تتشارك و تتحمل مسؤولية حماية الصحة ورفاهية سكانها.

3-الامن الشخصي:يمكن تعريفه بانه مجموعة من الاجراءات التي يتوجب على كل فرد اتخاذها ومراعاتها لحماية نفسه حماية تامة من خلال وعيه ومعرفته بمفاهيم الامن بشكل عام واساليب الخصوم في التاثير على العنصر البشري بشكل خاص.

4- الامن المجتمعي:يقصد به حصيلة كافة الاجراءات اللازمة لحماية المجتمع ضد كل عائق يعيق من تقدمه وتحقيقه لاهدافهبالامكانات والقدرات المتاحة، ويكون الامن المجتمعي من مسؤولية الدولة فهو مجموعة الخطط والتدابير التي تتخذها الدولة لحماية وتامين سكانها ،عن طريق الاستغلال الامثل لطاقاتها ومواردها لتامين الحياة الكريمة لمواطنيها .

5- الامن السياسي :هو ضمان تامين الحاجة الى التحرر من الخوف والحاجة وضمان تامين الحماية من تهديد القمع السياسي والحماية من التعرض للصراعات والحروب والهجرة للمواطنين كافة وفي الوقت ذاته ودون استثناء .

6-الامن الاقتصادي: ويشمل الانشطة والتدابير التي تؤهل الانسان للحصول على احتياجاته الاساسية من الماكل والملبس والسكن والعلاج ،لاسيما في الظروف الاستثنائية كالكوارث الطبيعية والحروب والازمات الاقتصادية وضمان الحد الادنى لمستوى المعيشة[1].

7- الامن السيبراني :وهو مجال من مجالات تكنولوجيا المعلومات وتتم فيه حماية الافراد والمؤسسات والانظمة من حالات الاختراق الرقمي او الدخول غير المصرح به او التهديدات الامنية الخطيرة ،التي من شانها ان تؤثر على خصوصية البيانات والمعلومات ،وقد كان الهدف الرئيس لظهور الامن السيبراني ظهور الهجمات الرقمية الخطرة والقيروسات التي يتم من خلالها مهاجمة الانظمة الرقمية الخاصة بالافراد والمنشات والسيطرة على ما تمتلكهمن بيانات حساسة وتعرضها للابتزاز والسرقة والتخريب المتعمد للمعلومات،كل ذلك كان سببا في ظهور الامن السيبراني لا بهدفف الدفاع او الحماية فقط وانما بدافع الوقاية ايضا وذلك من خلال القيام بهجمات متعمدة واكتشاف الثغرات الموجودة والعمل على اصلاحها فورا ،وهناك عدة مفاهيم ترتبط بالامن السيبراني كالجريمة الاكترونية،الهجمات الالكترونية وفيها يتم التخطيط غير القانوني للسيطرة على جهاز او نظام تابع لفرد او مؤسسة باستخدام التكنولوجيا الرقمية واجهزة متطورة او من خلال استغلال الثغرات الموجودة في اي نظام او استغلال جهل المستخدم وضعف ثقافته التكنولوجية.

من الجيد ان نستفيض هنا في مفهوم الامن السيبراني ،اذ شهدت الساحة الدولية تطورات خطيرة وسريعة هددت الامن الدولي وغيرته من مفهومه الصلب الى الامن الناعم الرقمي واللاتماثلي ،واصبحت حماية الدولة في منظومتها الاليكترونية او السيبرانية جزءا لايتجزا من امن الدولة القومي.فالامن السيبراني يعد من التحديات الامنية المعاصرة التي واجهت اشكالات كثيرة في فهمها ومسايرتها ولاسيما بالنسبة للدول ،الامر الذي جعلها بعدا مفاهيميا جديرا بالدراسة والبحث اكاديميا ومعرفيا ،وايجاد بروتوكولا معرفيا يسهل على صانعي القرار ايجاد الحلول اللازمة في حال تعرضه لاي اختراق،لاسيما وان العراق اصبح من بين الدول التي دخلت ولو على نطاق ضيق في مصاف الادارة الاليكترونية والعالم السيبراني،الامر الذي يترتيب عليه ان تتبنى الدولة اصلاحات واستراتيجيات امنية لحماية امنها السيبراني ،وتباينت تعريفات الامن السيبراني شانه

1 عادل عبد الحمزة ثجيل،الامن القومي والامن الانساني،دراسة في المفاهيم ،مجلة العلوم السياسية،العدد2016،51،ص332-334

كشان اي مصطلح جديد اخر اذ تناوله كل من منظوره ،فمثلا عرفه ليثو مارتي و نيتانماكي في كتابهما الموسوم (الامن السيبراني) بانه مجموعة من الاجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكومبيوتر وعواقبها وتنفيذ التدابير المضادة المطلوبة،فيما عرفه ادوارد اموروس على انه وسيلة من شانها العمل على تقليل الهجوم على البرمجيات او اجهزة الحاسوب او الشبكات

خصائص الامن السيبراني:- للامن السيبراني خصائص متعددة يمكن توضيحها بما ياتي

-الحماية من التهديدات الداخلية التي تعد واحدة من اهم مميزات الامن السيبراني فقد تتعرض المعلومات الى الهجوم الاليكتروني بسبب ضعف ثقافة المستخدمين في هذا المجال او بسبب جهله بامن المعلومات ،وفيه يتم السماح ببرامج مجهولة المصدر بالتفعيل او القيام باستخدام ادوات تمس الامن الشخصي للمستخدم ،او احتواء الادوات التي يتم استخدامها على فيروسات ضارة لايجب ان يحتوي عليها نظامه،وهنا ياتي دور الامن السيبراني بسرعة تنبيه الفرد او المؤسسة بالخطر ومنع وقوعه في اسرع وقت.

-الرؤية الشاملة،اذ تمنح وسائل الامن السيبراني لمستخدميها سواءا كانوا افراد او شركات رؤية شاملة على نقاط الضعف والقوة في انظمتهم ومن خلال ذلك يكون بامكانهم معرفة الثغرات التكنولوجية وحلها باسرع وقت وابداء المقترحات الخاصة بالطرق المثلى لمنع تكرار او حدوث تلك الثغرات مجددا.

-الحماية من التهديدات الخارجية،اذ يتم بناء جدار حماية قادر على تصفية المخاطر الخارجية الناتجة عن التعامل مع العالم الرقمي بدءا من الرسائل الاليكترونية الخطرة والضارة والفيروسات حتى معالجة الضعف في النظام .

-المراقبة المستمرة فجدران الحماية لاتعمل في وقت محدد وتتوقف ،بلتعمل باستمرا لغرض الكشف عن اي ثغرة او خلل والعمل على التعامل معه ومعالجته بالسرعة الممكنة.

-الامتثال للقوانين والسياسات اذ لا يتيح لمصادر خارجية الاطلاع على ما يتم مشاركته من معلومات وبيانات،او اساءة استغلالها باي صورة كانت

-التنوع اي انه يمتلك حلولا متنوعة ومتعددة فيما يخص معالجة مشاكل الامن السيبراني ،كما ويتعامل مع كافة انواع التهديدات المهددة لسلامة وامن المعلومات[1].

ومن وجهة نظر الباحثة فالامن السيبراني يعني الاستراتيجية التي تقوم بها الدولة لحماية انظمتها وبرامجها الالكترونية ومعلوماتها الحساسة من الهجمات الالكترونية وحمايتها من الاختراق او من الوصول اليها من قبل بعض الجهات التي تنوي تغييرها او اتلافها او استخدامها كوسيسلة للابتزاز مقابل مبلغ مادي اومقابل تقديم بعض التنازلات التي تمس سيادة الدولة.

خلاصة ما تقدم فالامن السيبراني يعد احد اهم انواع الامن الانساني فهو رغم حداثته قياسا بانواع الامن الانساني الاخرى،الا انه وفي الاونة الاخيرة تزايدت اهميته لما له من علاقة بسيادة وامن

1 عبد الرحمن عاطف ابوزيد،الامن السيبراني في الوطن العربي دراسة حالة المملكة العربية السعودية ،المركز العربي للبحوث والدراسات ،بحث منشور بتاريخ 6\4\2020 متاح على الموقع
http://www.acrseg.org /list.aspx?r =24734.

الدولة فالدولة التي لا امن سيبراني لها لا سيادة لها والدولة التي لا تستطيع ان تحمي امن ومعلومات مؤسساتها ومواطنيها من ان يوصل اليها او الدولة التي تكون غير قادرة على مواجة والتصدي لهجمات الامن السيبراني تعد دولة ضعيفة ممكن ان تقتحم معلوماتها بسهولة .

مؤشر الامن السيبراني ومكانة العراق في مؤشر الامن السيبراني

وما دمنا في صدد دراسة الامن السيبراني لايفوتنا ان نشير الى مسالة مهمة وهو مكانة العراق في مؤشر الامن السيبراني ،اذ عمل الاتحاد الدولي للاتصالات على انشاء مؤشر للامن السيبراني على المستوى العالمي لاول مرة عام 2015 بغية قياس مدى التزام 193 دولة عضوا في الاتحاد الدولي للاتصالات بمرتكزات الامن السيبراني مساعد الدل من خلال زيادة الوعي بحالة الامن السيبراني في جميع انحاء العالم من خلال تحديد مخاطر الامن السيبراني ،وفي عام 2021 صدرت احصائية لمؤشر الامن السيبراني العالمي لكل من الركائز الاتية وتشمل القانونية –التقنية-التنظيمية-تنمية القدرات –التعاون ومن ثم تقييم التزام الدولة عن طريق استبانة على الانترنت الامر الذي ساعد على جمع البيانات اللازمة وبالتشاور مع مجموعة خبراء تم ترجيح هذه الاسئلة للوصول الى مجموع نقاط المؤشر والجدول التالي يوضح الدول العشرة الاكثر قدرة عى مواجهة المخاطر السيبرانية في العالم.

جدول (١) الدول العشر الاكثر قدرة على مواجهة التهديدات السيبرانية

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسة
سنغافورة	0.95	0.96	0.88	0.97	0.87	0.92
الولايات المتحدة الامريكية	1	0.96	0.92	1	0.73	0.91
ماليزيا	0.87	0.96	0.77	1	0.87	0.89
سلطة عمان	0.98	0.82	0.85	0.95	0.75	0.87
استونيا	0.99	0.82	0.85	0.94	0.64	0.84
موريشيوس	0.85	0.96	0.74	0.91	0.70	0.82
استراليا	0.94	0.96	0.86	0.94	0.44	0.82
جورجيا	0.91	0.77	0.82	0.90	0.70	0.81
فرنسا	0.94	0.96	0.60	1	0.61	0.81
كندا	0.94	0.93	0.71	0.82	0.70	0.81

المصدر\تغريد معين حسن المشهدي،الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة،مجلة البحوث الجغرافية ،العدد20،ص249.

اما بالنسبة للدول العربية الاكثر مواجهة للامن السيبراني فتتصدر القائمة ثلاثة دول يبينها الجدول رقم(2) فتتصدر عمان القائمة تليها مصر ،ثم قطر.

جدول رقم(2) المراكز الثلاثة الاولى للدول العربية الاكثر مواجهة للامن السيبراني

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسة
عمان	0.98	0.82	0.85	0.95	0.75	0.87
مصر	0.92	0.92	0.4	0.92	0.7	0.77
قطر	0.83	0.82	0.65	0.78	0.33	0.67

المصدر\تغريد معين حسن المشهدي،الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة،مجلة البحوث الجغرافية ،العدد20،ص250.

اما فيما يخص العراق فيعد من الدول التي تواجه تحدي سيبراني بمجالاته المختلفة ولاسيما المجال الامني ،اذ لايزال لا يمتلك القدرات التي تؤهله للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني ،فمع التحول السريع للمجتمعات من الفضاء الحقيقي الى السيبراني وجد العراق نفسه يدخل الى هذا الفضاء اللامتناهي والسريع دون المرور بمرحلة انتقالية فالمقومات المادية والبشرية العراقية لاتزال غير قادرة على التفاعل ايجابيا مع هذه التحديات العديدة للفضاء السيبراني ،فالبلد بحاجة الى جهد معرفي واداري وقانوني وتقني ليكون قادرا قادر على التاثير في المجال الامني السيبراني من ناحية ومن ناحية اخرى يكون قادرا على حماية امنه من التهديدات السيبرانية،شغل العراق عام 2018 المركز 107 عالميا و13عربيا وتراجع عام 2022 الى 129 عالميا من اصل 184 و17 عربيا،ويمكن ارجاع سبب هذا التراجع الى اسباب عديدة هي:-

أ-تراجع دور فريق الاستجابة للاحداث السيبرانية وهو فريق وطني مشترك مختص بمجال الامن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للانترنت ونشر الوعي في مجال الخصوصية والحماية الذاتية للافراد والمؤسسات على الانترنت يعمل تحت اشراف مستشارية الامن القومي العراقي .

ب-قانون جرائم المعلوماتية لم يصوت عليه رغم القراءة الاولى وتبدل نسخه عدة مراتبطريقة تثير مخاوف على الحريات العامة.

ج-عدد المؤتمرات وورش العمل والندوات عن الامن السيبراني محدودة جدا مقارنة مع دول الجوار مثل السعودية .

د-الاموال المخصصة للامن السيبراني قليلة مقارنة مع دول الجوار ومنها ايران التي خصصت مليار دولار سنويا في مجال الامن السيبراني .

ه-لا توجد بنية تحتية ومادية متكاملة في مجال الامن السيبراني [1].

1 باسم علي خريسان ،الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020،مركز البيان للدراسات والتخطيط ،2021،ص10،8،4

المحور الثاني :اثار الامن السيبراني على الامن الوطني العراقي:

قبل الولوج بتفاصيل اثار الامن السيبراني على الامن الوطني في العراق ،لابد من الاشارة الى انواعه ،فهو يشمل انواعا متعددة يمكن بيانها بالاتي[1]:

أ-الامن السحابي :بعد التوجه العالمي في الاونة الاخيرة الى استخدام تكنولوجيا الذكاء الاصطناعي والسحابات التخزينية ،اصبح تامين السحابة الرقمية امرا لابد منه لاحتوائها كميات هائلة من البيانات التي تمس امن المؤسسات والدول وهنالك مجموعة من الشركات التخصصة خدمات في هذا المجال مثل شركة كوكل كلاود ومايكروسوفت .

ب-امن الشبكات نظرا لكون معظم الهجمات تحدث عبر الشبكات الالكترونية،فقد تم وضع انظمة امنية تزيد من مستوى الامان للشبكات مع ضمان حلولا فورية وتحكم كامل في عناصر البيانات والوصول للشبكة كي تمنع اي هجمة او اختراق البيانات المخزونة على خوادمها.

ج-امن التطبيقات من المعلوم ان تطبيقات الويب متصل مباشرة بشبكات الانترنت وعليه فانها بلا شك تكون عرضة للتهديد بالهجمات السيبرانية ،ويساعد هذا النوع من الامن السيبراني الشركات والمؤسسات باكتشاف البيانات الحساسة التي يكون من المفترض حمايتها من الهجمات المتوقعة عن طريق برامج مضادة للفيروسات وجدران حماية ،فضلا عن عمليات تشفير معلوماتها.

د-امن الامعلومات والبيانات :هو تصميم ونشر الادوات الخاصة بحماية معلومات العمل الشخصية من التدمير او التعطيل وحتى التغيير ،وتم تصميم هذا النوع من الامن السيبراني للحفاظ على سرية وتوافر وسلامة بيانات العمل ،فهو يضمن فقط للتطبيقات والانظمة المصرح بها من الموصول الى تلك المعلومات ،كما ويعمل على مراقبة والتحقيق في السلوك الضار المحتمل لاحتواء التهديدات المحتملة والتعامل كعها بشكل ايجابي وفوري.

ه-امن البنى التحتية:الذي هو اجراء امني مهمته حماية البنى التحتية الحيوية للنظام وحمايتها من الفساد والتخريب والارهاب كاتصالات الشبكة او مركز البيانات او مركز تكنزلوجيا المعلومات او الخوادم.وفي هذا النوع من الانمن يتم وضع خطة طواريء في حالة استهداف الانظمة لدى الشركة من قبل منفذي الهجمات الاليكترونية وتشمل البنية التحتية التي يقوم بحمايتها كل من (انظمة امداد ونقل الطاقة،امدادات المياه،انظمة التبريد،التدفئة ودوران المياه).

و-امن المستخدم النهائي :هو ممارسات تقنية تستخدم لحمايةاجهزة المستخدمين النهائيين كالهواتف المحمولة واجهزة الحاسوب والتي يستخدمها الموظفون في الولوج بشبكات الشركة من الهجمات السيبرانية الناتجة عن البرامج الضارة وغير المرغوب فيها كالهواتف ،وتسعى المؤسسات الى حماية هذه الاجهزة لصد اي محاولة خارجية للوصول الى الشبكات وقواعد البيانات المخزونة على خوادم هذه الشركات او المؤسسات.

ز-امن انترنت الاشياء كالاجهزة الذكية والمستشعرات الحساسة وادوات الذكاء الاصطناعي ،وبالرغم من فوائدها الانتاجية الا انها تعرض المؤسسات للتهديدات الاليكترونية ،ويتمثل دور هذا النوع من الامن السيبراني بحماية هذه الاجهزة من خلال اكتشاف الاجهزة المتصلة وتصنيفها

1 ايهاب خليفة،القوة الالكترونية كيف يمكن ان تدير الدول شؤونها في عصر الانترنت ،مطبعة العربي،القاهرة،2017،ص113

بحسب دورها التشغيلي ،ومدة الصلاحية الممنوحة للوصول الى قاعدة البيانات ،فعند استشعار اي حركة مريبة او غير مالوفة يقوم بالتحكم في انشطة الشبكة الموجود عليها ومراقبة اي عملية استغلال لتلك الاجهزة والتعامل معها فورا.

ح-التعافي من حالات الكوارث المتعلقة بالهجمات الاليكترونية او الاسباب الطبيعية :هو استئناف الاعمال بعد عمليات التخريب في قواعد البيانات وفيه يتم وضع خطط متعددة لمساعدة الموظفين على التواصل ووالاستمرار في اداء وظائفهم في حالة حدوث اي هدوم اي التعرض لاي كارثة طبيعية.

اما انواع الجرائم او التهديدات او المخاطر السيبرانية (هي احتمال وجود تهديد وهشاشة داخل الفضاء الالكتروني للبلد يضر بامن وسلامة نظم المعلومات وهياكل البنية التحتية المعلوماتية الرئيسة) التي من الممكن ان يتعرض لها الافراد او المؤسسات او الدول فهي :

أ-الجريمة ذات الصلة بالحاسوب

ب-جرائم غسيل الاموال والجرائم الاقتصادية

ج-الجرائم الارهابية السيبرانية

د-جرائم ضد الاشخاص

ه-القرصنة

و- واخيرا جرائم متنوعة تشمل انشطة التجسس والتخابر والابتزاز والتهديد.

اما مصادر التهديد السيبراني فهي الدول الاجنبية والنقابات الجنائية المنظمة ، الارهابيين والجماعات المتطرفة ، والهاكرز، الشركات[1].

وبعد اطلاعنا على انواع الامن السيبراني وانواع الجرائم او التهديدات السيبرانية تبين لنا انها تمس جوانب الحياة المختلفة للافراد والمؤسسات والدول وهذا يعني انها تمارس دورا ليس بالقليل على امن الدولة وان ما يمكن تاكيده في هذا البحث هو ان العراق اصبح يولي للامن السيبراني اهمية واسعة ،لا سيما لدى المؤسسات والاجهزة الامنية كونه مطلبا ضروريا لكافة الدول دون استثناءومطلبا متزايد الاهمية بالنسبة للدول التي قامت بتوظيف البعد التكنولوجي الرقمي والافتراضي في تسيير شؤونها العامة على الصعيد المحلي والاقليمي والدولي و اصبح محط اهتمام النخب السياسية وصانعي القرار،اما عن الابعاد او الاثار التي تنتج عن الامن السيبراني في العراق فيمكن القول بان الامن السيبراني له علاقة وثيقة بالجغرافية السياسية للدولة وعناصر قوتها ،فهو يطال المقومات السياسية والاقتصادية والاعسكرية والاجتماعية والانسانية للدولة وهذه كلها تعد ضمن عناصر قوتها،ولكن قبل الاشارة الى هذه الابعاد سنعطي لمحة عن انعكاس الامن السيبراني على الفضاءات الرقمية العراقية في مواجهة المخاطر السيبرانية من خلال تكييف المنظومة الامنية مع التحولات الجيوستراتيجية الاقليمية والعالمية ،اذ ان التهديد السيبراني اصبح من القضايا الهامة بالنسبة للامن الوطني العراقي ،لذا من الواجب دعم استراتيجية الامن والدفاع العراقية ،وتكييفها

1 تغريد معين حسن المشهدي،الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة،مجلة البحوث الجغرافية ،العدد20،ص248

مع المتطلبات المستقبلية لمواجهة كافة التهديدات حسب خطورتها والعمل على بناء منظومة قادرة على التكيف مع احتمال ما يمكن ان يقوم به المهاجمون وتتمثل ابعاد الامن السيبراني على الامن الوطني العراقي بما ياتي:-

1-البعد السياسي للامن السيبراني في العراق:-تشكل السياسة كما معروف عصب حياة الدول والمجتمعات ،وبسبب التطور التكنولوجي تحولت الصراعات السياسية من ارض الواقع الى الواقع الافتراضي ،لا سيما في السنوات الاخيرة اذ اصبح توظيف القوة السيبرانية يعد سلاحا مهما وناجحا للتغلب على الخصوم السياسيين ،عن طريق تنفيذ اجندات خاصة تتمثل بضرب المنظومة التكنولوجية للدولة.

2- البعد الاقتصادي والتوجه نحو الاقتصاد الرقمي اذ اصبح العراق من الدول التي تعمل على تطوير قدراتها العلمية والسيبرانية في الجانب الاقتصادي من اجل تجنب اي محاولة اختراق ،لاسيما في ظل الصراعات والتوترات الاقليمية مما يجعل العراق يركز ويهتم بشكل كبير على الحفاظ على امنه الاليكتروني والسيبراني داخل مؤسساته الرسمية ومكافحة الجرائم الاليكترونية التي غالبا ما تاتي من قبل دول تختلف في توجهاتها وايديولوجياتها مع العراق،وعلى صعيد البورصة والتداول المالي من خلال حماية رقم الاعمال التي يحوز عليها العراق ،مما جعل الامن السيبراني في هذا المجال يرتبط ارتباطا وثيقا بالدرجة الاساس بامن الدولة ومن ثم بالامن الاقتصادي.

3-البعد الاجتماعي وتامين منصات التواصل الاجتماعي من المخاطر الخارجية :-فقد عملت منصات التواصل الاجتماعي على خلق فضاء تواصلي غير مسبوق مما جعل فرصة المخترقين ترتفع من خلال البحث عنهم واستخداهم بتصميم برامج مضادة ضد الهيئات والمؤسسات وفتح باب الحروب الافتراضية الوادة لاسيما اذا كانت تلك الدولة تتمتع بتنوع اثني ،وان مشاركة جميع افراد هذه الاثنيات في هذه الحروب يشكل خطرا على وحدة الدولة وتماسكها ،زعليه لابد من العمل على توعية المواطنين بهذه المخاطر لتحقيق الامن السيبراني الاجتماعي.

4- البعد العسكري للامن السيبراني :-الحروب المعلوماتية قديمة قدم الانسان وبقيت الدوافع الكامنة ورائها دون تغيير والتي تتمثل تقويض ثقة الخصم وتعطيل خطوط اتصالاته وارباكها وخلق الاوهام في نفسه بشان طبيعة ومسرح النزاع وبقيت هذه الدوافع حتى يومنا ههذا،الا ان الذي تغير هو طريقتها ولاسيما في القرن الحادي والعشرون وما تزامن معه من تطورات في البنى التحتية المعلوماتية فاصبحت الحروب المعلوماتية في الوقت الحاضر تتميز بعدة مميزات هي:-

-تتمتع بكونها هجمات شرسشة قادرة على تمزيق النسيج الاجتماعي وضرب المنظومة المجتمعية والقيمية داخل البلد المستهدف.

- بامكان الجهات الفاعلة غير الحكومية المشاركة في هذه الحروب.

-من المحتمل ان تنشأ حالة من النزاع الدائم منخفض المستوى وهو ما يسمى بالحرب الباردة السيبرانية ضمن هذا النوع من الحروب .

وقد عمل الاستخدام الاستخدام التكنولوجي المكثف للمعلومات الجديدة على تعزيز القدرات القتالية للاسلحة التقليدية والتكنولوجيات العسكرية الاخرى ،ومن هذا المنطلق ينظر العسكريون الى

تكنولوجيا المعلومات على انها سلاح وهدف في الوقت ذاته ،فعسكريا تقع العمليات التي تتم للحصول على تفوق المعلومات ضمن نطاق حروب المعلومات ،وهذا هذا النطاق نفسة تتم عملية شن المعلومات الدفاعية والهجومية عن طريق التدخل المسلح والحروب الاليكترونية وغيرها .

وما دمنا في صدد الحديث عن البعد العسكري والحروب ودور الامن السيبراني فيها ،فيمكن القول ان الهجمات السيبرانية العسكرية او الحروب السيبرانية تتم من خلال اربعة مستويات اومراحل هي: المرحلة الاولى جمع المعلومات الاستخبارية،الثانية هي العمليات التي تستهدف المعنويات (الحرب النفسية)،اما المرحلة الثالثة فهي عمليات هجومية،واخيرا العمليات الدفاعية.

وعليه فان الحروب السيبرانية تعني قيام دولة او فواعل من غير الدول بشن هجمات اليكترونية قد تكون من طرف واحد او متبادلة ومما تتميز به هذه الحروب عن الحروب العسكرية التقليدية بان الحروب العسكرية تبدا باعلان واضح وصريح لحالة الحرب وتستخدم جيوشا نظامية في ميدان قتال ومعارك محدد ومعروف ،بينما الحروب السيبرانية او هجمات الفضاء الالكتروني لا يحدها زمان او مكان ولا سبقها اعلان وغامضة الاهداف والفاعلين لانها تكون عبر شبكات المعلومات والاتصالات عابرة الحدود الدولية ،كما انها تلجا الى استخدام التكنولوجيا والاسلحة الاليكترونية الحديثة التي تتوائم مع التطور التكنولوجي ،اذ توجه هذه الاسلحة ضد المنشات الحيوية او تدس عن طريق عملاء لاجهزة الاستخبارات ،فضلا عن ذلك فان هذه الحروب لا يتعرف بها علنا خشية من ان الاعتراف بها يتطلب من الطرف الاخر المواجهة والانتقام ،والخوف من ان تتطور الى حربا تقليدية وتتميز الحروب السيبرانية بمميزات عديدة وكما يأتي[1]:

1- من مميزاتها عدم القدرة على اسناد المشكلة في دولة ،اذ يتمكن المهاجمون من اختراق الخوادم في اي بقعة في العالم ويمكن تحديد انشطتهم في اي منطقة جغرافية ويمكن ان يكتبوا باي لغة.[2]
2- من مميزات هذه الحروب عي ميزة الانكار ،اي عندما يكون من غير الممكن اثبات الجانيب علنا ،فان من السهل على المشتبه به ان ينكر من باب (انك تعلم اننا فعلناها،لكنك لا تستطيع ان تثبت ذلك) ،فعلى سبيل المثال في الانتخابات الامريكية لعام 2016 ونتيجة النفي المتكررلحدوث اي خروقات فيها اقترح فلاديمير بوتين في النهاية انه كان من الممكنت ان يكونوا قراصنة روسيين ،لكنه اكد انه ليس له علاقة بالحكومة الروسية.
3- التصعيد وذلك من خلال الدعايات والاخبار المزيفة والتشويش وغيرها.

وتعد الحروب السيبرانية نوع جديد من الحروب و ساحة معركة خامسة ،فالحروب السيبرانية يمكن ان تجري بصورة واسعة في الفضاء السيبراني باستخدام واستهداف التكنولوجيا المعلوماتية والاتصالات ،والاعتماد على الشبكات الذكية وغيرها من انظمة المراقبة والرصد عن طريق الانترنت ،وتضع مركز موارد الطاقة والنقل والدفاع في متناول الذين يسعون الى احداث الفوضى في الحكومة وبين السكان المدنيين.

1 جانكارلوأ.بارليتا،ووليام أ.بارليتاوفيتالي تسيجيشكو ،النزاع السيبراني والاستقرار الجيوسيبراني،البحث عن السلام السيبراني،الاتحاد الدولي للاتصالات،2011،ص51
2 سمير قلاع الضروس،الامن السيبراني الوطني:قراءة في اهم الاستراتيجيات الامنية والتقنية لمواجهة الجريمة الالكترونية في الجزائر،مجلة الرواق للدراسات الاجتماعية والانسانية،المجلد8،العدد2،2022،ص254

ويمكن ايجاز مخاطر وابعاد الامن السيبراني على العراق بالنقاط التالية[1]:-

1- ان وجود اقتصاد رقمي في البلد يعتمد على الاداء الفاعل للبنى التحتية الرقمية ،ففي الفضاء السيبراني البلد ليس معزولا عن غره من البلدان،لكنه مترابط معها،عن طريق شبكات مترابطة للبنى التحتية للمعلومات ،وعليه فان البلد يكون عرضة للمخاطر التي قد يتنبأ ببعضها .

2- هناك جهات فاعلة ذات نوايا غير مشروعة او شريرة داخل الشبكة العالمية للشبكات ،ومع وجود عيوب هيكلية ،فان ذلك يجعل من الممكن لتلك الجهات استغلالها لاغراض خبيثة او سيئة ضد البلد من اجل المساس بسرية نظم المعلومات الوطنية والبنية التحتية الحيوية للمعلومات ،الامر الذي ينعكس سلبا على المواطن والامن الوطني للبلد.

3- يمكن استخدام مواطن الضعف في الفضاء السيبراني لاستغلال المصالح الاقتصادية الوطنية ،مما يشكل خطرا يهدد الامن القومي ومن امثلة هذه التهديدات (العمليات التخريبية التي اصابت بعض المواقع الحكومية،زيادة صناعة الجرائم السيبرانية،الممارسات الاحتيالية،التجسس الالكتروني المنسق،سرقة الاصول الفكرية،الجرايم المالية عبر الانترنت،جرائم غسيل الاموال،الارهاب الالكتروني ،الصراع والعنف المستمر على الانترنت،اساءة استغلال وسائل الاعلام ووسائل التواصل الاجتماعي لشن حملات مغرضة ضد الدولة،القرصنة الالكترونية والتدخل الخبيث في انظمة الكومبيوتر والانظمة الرقمية الاخرى). وكل هذه التهديدات لا تنسجم مع سياسة الرفاهية لاي دولة ولها اثار على كافة مجالات الحياة فيها.

ومن خلال الابعاد التي اشرنا اليها اتضح لنا اهمية الامن السيبراني بالنسبة للبلد وامنه القومي وسيادته فاي اختراق لاي من هذه الابعاد او جميعها فان ذلك سيؤدي الى المساس بوحدة البلد وضرب منظومته المجتمعية وضرب اقتصاده الوطني ويعمل على تفككه والمساس بسيادته.

المحور الثالث :السبل والامكانات المتاحة للحد من الهجمات السيبرانية

المطلب الاول :المنظومة التقنية للحد من الهجمات السيبرانية المتعلقة بالامن السيبراني في العراق :- ما دمنا في صدد دراسة طرق معالجة الهجوم السيبراني ،لابد اولا من الاشارة الى التقنيات التي يتم من خلالها موجهة هذه الهجمات و هنالك عدد من التقنيات الخاصة بمعالجة خطر التهديدات السيبرانية :

1-جدران الحماية ويسمى ايضا بالجدار الناري وهو جهاز او برنامج يفصل بين المناطق الموثوق بها داخل شبكات الحاسوب،ويكون عبارة عن برنامج على جهاز حاسوب اخر يقوم بمراقبة العمليات المارة عبر الشركة ويقوم برفضها او السماح لها وفق ضوابط محددة وله انواع مختلفة هي:

1 استراتيجية الامن السيبراني العراقي،مستشارية الامن الوطني،امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات،ص2

أ- proxy firewall هو اقدم انواع جدران الحماية و يعمل كبوابة دخول بين شبكة واخرى لتطبيق معين وخوادم البروكسي بامكانها القيام بوظائف اخرى كتخزين المحتوى المؤقت ومنع الاتصالات المباشرة من خارج الشبكة.

ب- Firewall يسمح هذا النوع بحجب حركة مرور البيانات او الاتصالات مستندا على عوامل متعددة،كالحالة والناقل والبروتوكول ،فضلا عن مراقبته لجميع الانشطة منذ اللحظة الاولى لبدء الاتصال حتى نهايته .

ت- Stateful Inspection Unified Threat Managementيمثل مركز الادارة للتعامل مع التهديدات ويجمع بين وظائف الجدار الناري التفتيشي وبرامج مضادات الفيروسات ،فضلا عن ادارة الخدمات السحابية .

ث- generation Firewall- NEXT هي جدران نارية اكثر تطورا من سابقاتها لا يقتصر عملها على تصفية الحزمات او تفتيش الحالة،اذ تقوم اغلب الشركات باعتماد هذه الانواع المتطورة من جدران الحماية لحجب التهديدات الحديثة كالبرلامج الضارة المتطورة والهجمات على التطبيقات.

ويمكن القول ان جدران الحماية رغم فائدتها ،الا انه يعترض استخدامها بعض القيود والمشاكل،فهي غير فعالة بشكل تام للتصدي لكافة انواع الهجمات الاليكترونية،ففي الوقت الحاضر تعلم المتسللون الماهرون كيف ينشئون بيانات وبرامج تخدع جدار الحماية وتخترقه.

2- برامج مكافحة الفيروسات

3-خدمات البنية التحتية للمفاتيح العمومية التي تضم الترتيبات التي يتم بها ربط المفتاح العام مع المستخدم بواسطة مصدر الشهادة (هوية المستخدم) التي لابد ان تكون فريدة لكل مصدر شهادة ويتم ذلك عن طريق برمجيات خاصة في مصدر الشهادة ،التي قد تكون تحت اشراف بشري الى جانب برمجيات منسقة في مواقع مختلفة ومتباعدة .

4-خدمات الكشف المداراة :- نظرا لكون مرتكبي الجرائم الالكترونية والبرامج والتقنيات التي يستخدمونها اصبحت اكثر تعقيدا وتطورا،فقد اصبحت هناك ضرورة ملحة للشركات الاستثمار في اشكال دفاعية اكثر قوة وامانا،فمنذ عام 2018 لم يعد مجرد وجود دفاعات قادرة على التفاعل مع التهديدات امرا كافيا،بل اصبح من الضروري وجود دفاع استباقي بامكانه تحديد الهجمات الالكترونية قبل حدوثها .

5-اختبار الاختراق :-يعد هذا الاختبار خطوة مهمة للتحقق من مدى فاعلية انظمة الامان،اذ يقوم هذا الاختبار على محاكاة الهجوم الذي قد تواجهه المؤسسات او الدول او الافراد،ماختراق كلمة المرور والتصيد الاحتيالي فبمجرد اجراء الاختبار سيقدم المختبرون نتائجهم والمساعدة من خلال التوصيات والمقترحات بالتغييرات المحتملة على النظام.

6- تدريب الموظفين:-يعد تدريب الموظفين او نشر الوعي الخاص بالامن السيبراني داخل الدولة ومؤسساتها امرا لا يقل اهمية عن التقنيات السابقة،فوجود مجتمع على دراية بمخاطر الهجمات السيبرانية ويعي دوره في مواجهة هذه الهجمات احد اشكال الدفاع ضدها ومواجهتها ويتم ذلك من خلال نشر الوعي السيبراني بين افراد المجتمع من خلال اقامة الورش والندوات الخاصة بهذا الموضوع،ومؤخرا تمفتح العديد من الاقسام العلمية الخاصة بالامن السيبراني في الجامعات

العرافية،فضلا عن فتح باب التقديم للطلبة المتخرجين من المرحلة المتوسطة بفرع خاص في الفرع المهني اطبق عليه الامن السيبراني،وهذه البوادر تدل وبشكل واضح بان بلدنا قد بدا باتخاذ الخطوات الصحيحة اللازمة لانشاء جيل متعلم ومتخصص في هذا المجال المتزايد اهمية وخطورة.

المطلب الثاني: الاستراتيجية العراقية للامن السيبراني

المقصود باستراتيجية الامن السيبراني بانها خطة عالية المستوى تعمل على المساعدة في تحديد كيفية تامين المؤسسات خلال السنوات الثلاث او الخمسة القادمة متضمنة تحولا من العمل على نهج الامان التفاعلي الى نهج الامان الاستباقي ،اذ تركز لاستراتيجية بشكل اكبر على منع الهجمات السيبرانية بدلا من الرد عليها بعد حدوثها.وان الضعف في اجراءات الامن السيبراني في العراق يوازي خطر الارهاب ،وكما اشرنا سابقا الى التهديدات او الجرائم السيبرانية المهددة للامن الوطني وتعد مخالفة لاستراتيجية الامن الوطني لاي دولة كانت ،ولها قدرة على احداث ضرر كبير على البلد ،وتكمن الايديولوجية الاساسية للاستراتيجية الوطنية للامن السيبراني في تقديم اطر واليات ذات صلة بمهارات معالجة التهديدات السيبرانية ويمكن القول بان وضع استراتيجية وطنية للامن السيبراني في العراق يعمل على :-

1-تقييم مواطن الضعف الوطنية وتشمل

- الكشف عن الثغرات والمقصود بها الضعف الهيكلي لنظم معلومات البلد والبنية التحتية الحيوية للمعلومات التي تتراوح بين العيوب التقنية والتدابير غير المدروسة والاهمال البشري.

-اجراء تقييم سنوي على مستوى الدولة بهدف الكشف عن نقاط الضعف في نظم المعلومات الحكومية والمواقع الشبكية،وعمليات معالجة البيانات ،فضلا عن الكشف عن مواطن الضعف الموجودة في البنية الاساسية للمعلومات الحيوية للبلد.

-التقييم المشار اليه اعلاه من شانه ان يعمل على تقدير مستوى عدم استعداد الدولة ومدى حاجتها الى حماية بناها التحتية المعلوماتية والبنى الاساسية للاتصالات.

- الهدف الرئيس من الاستراتيجية هو بناء اليات لاتخاذ الاجراءات المضادة التي تمكن البلد من معالجة الثغرات ومواطن الضعف في نظم معلوماتها

-هناك جهود تهدف إلى معالجة بعض هذه التحديات على المستويات الوزارية من خلال فريق الاستجابة للحوادث الاليكترونية العراقي. ومع ذلك، فإن استراتيجية الامن السيبراني العراقي تعمل على وضع الحجر الاساس لتنسيق النظام البيئي السيبراني في البلد مع إطار موحد للامن السيبراني

2-قياس الاثار والفرص

فبالنسبة للاثار يمكن القول بانه هناك العديد من المزايا المرتبطة بتنفيذ الاستراتيجية الوطنية للامن السيبراني. إن بناء ورعاية الثقة في استخدام نظم المعلومات الوطنية وتكنولوجيا المعلومات والاتصالات الحساسة أمر حاسم بالنسبة للرفاه االجتماعي والاقتصادي للمواطنين، ولذلك فانه من الضروري تأمين بلدنا في الفضاء السيبراني وبالتالي غرس مستوى عال من الثقة بين المستخدمين و الثقة في الاقتصاد الرقمي وفي الوقت الحاضر بدا العراق بالاعتماد على أداء تكنولوجيا المعلومات والاتصالات وتشغيل البنى التحتية للمعلومات الحيوية. وتعتمد تعاملاته في النقل

والاتصالات والتجارة الالكترونية والخدمات المالية على سرية المعلومات المتدفقةعبر هذه البنى التحتية وتكاملها ،وتوافرها ،تعمل كما وتعمل استراتيجية الامن السيبراني على اظهار بنية أمنية وطنية جديدة وشاملة عبر دمج الامن المادي والسيبراني كتدابير مضادة ضد التهديد الخارجي ،الامر الذي يعزز قدرة البلد على التاهب.

اما بالنسبة للفرص فان وجود البلد في المجال السيبراني فان هذا سيوفر له العديد من المزايا،منها الاقتصاد المرن وتحفيز الابتكارات والمشاركة الفعالة والتنميةوتدفق الاستثمار الاجنبي المباشر،كما ويوفر التواجد في هذا المجال فرصة للنهوض بالقدرات العسكرية،فضلا عن انه يهيء فرصة للعراق في الدفاع عن مواطنيه والحفاظ على عمليات البنية التحتية للمعلومات المهمة اثناء الهجمات الالكترونية التي لا يمكن التنبؤ بها.

- اهمية الاستراتيجية الوطنية للامن السيبراني:-

أ-طبيعة التهديدات السيبرانية المتنوعة الاخذة في التطور هي المحرك الرئيس لاستراتيجية الامن الوطني السيبراني الحالية الى ماهو ابعد من نطاقها الحالي.

ب-تشكل التهديدات الامنية الحالية كالجريمة السيبرانية والعنف والارهاب تهديد للاعتماد المستقبلي لبلدنا على الفضاء السيبراني لذلك لابد من وضع استراتيجية وطنية قادرة على مواجهة هذه التهديدات.

ج- تعمل الحكومة في الوقت الحاضر على الاستجابة باتجاه الحد من تاثير التهديدات السيبرانية وتصاعدها بطريقة تضمن وجود سيادة البلد.

نطاق الاستراتيجية العراقية للامن السيبراني:-تغطي هذه الاستراتيجية الاولويات الوطنية ،فضلا عن الاطار العام للشراكة والتعاون الدولي بشان الامن السيبراني وتغطي المجالات التالية:

-الحكومة الفعالة

-الاطار التشريعي والتنظيمي

-تكنولوجيا الامن السيبراني

-ثقافة الامن السيبراني وبناء القدرات

-البحث والاتطوير باتجاه الاعتماد على الذات

-الامتثال والتنفيذ

-الجاهزية لحوادث الامن السيبراني

-التعاون الدولي

تاسيسا على ما تقدم اصبح اليوم لزاما واكثر من اي وقت مضى ضرورة التركيز على العمل القضائي والتنسيق الامني والعسكري لمكافحة الجرائم الداخلية وتعزيز دور ثقافة الامن السيبراني ونشرها بين افراد المجتمع ،لاسيما في مجال حفظ انظمة المعلومات والامن السيبراني لدى منتسبي مؤسسات الدولة كمنتسبي جهاز المخابرات وجهاز الامن الوطني من خلال الاعتماد

على مجموعة من الاجراءات او الاستراتيجيات لتقوية المنظومة السيبرانية العراقية وذلك من خلال :

-الزامية تفعيل جدار الحماية من خلال البصمة الالكترونية والتوقيع الرقمي وتقوية انظمة الباسوورد وهذه كلها تقنيات تمنع الاختراق والتزوير من خلال تطبيق سياسة امنية عالية الدقة للمؤسسات والاجهزة التي تشير الى وجود مواقع ارهابية او اجرامية،لاسيما في المؤسسات الاقتصادية (؛البنوك والبورصات)والمؤسسات الرسمية التي تحوز على ارقام واحصائيات.

-العمل على وضع برامج خاصة للحماية من الفيروسات .

-تفعيل القوانين الخاصة بمرتكبي الجرائم الالكترونية والهاكرز داخل الدولة،اما على الصعيد الدولي فلابد ان تعمل الدولة على توقيع ما امكنها من اتفاقيات حماية الانظمة الرقمية والافتراضية داخل الدولة وفرض عقوبات دولية صارمة على مرتكبي تلك الجرائم

-العمل على خلق جيل رقمي ملم في مجال الامن السيبراني والثقافة السيبرانية ،من خلال توعيته باهمية وخطورة الابعاد المترتبة على الجرائم الالكترونية المتمثلة بالابعاد الامنية والسياسية والاقتصادية والاجتماعية.

الخاتمة

اولا :الاستنتاجات

1-للامن السيبراني ابعاد على الامن الوطني في العراق.

2-تتمثل ابعاد الامن السيبراني بالابعاد السياسية والاقتصادية والاجتماعية والعسكرية.

3-هنالك توجه ملحوظ من قبل الدولة نحو الاهتمام بالامن السيبراني والثقافة السيبرانية

ثانيا:-المقترحات

دخل النظام العالمي في الوقت الحاضر في حقبة جديدة تتمثل بالتطور السريع واللامتناهي في مجال تكنولوجيا المعلومات وهذا الامر يفرض على الدولة التفاعل والتكيف مع هذا التغير في الداخل والخارج لتحقيق المصالح الوطنية من خلال العمل على

1-حماية سرية بيانات الدولة

2-حماية البلد من ان يكون مرتع للجهات ذات النوايا السيئة الجماعات الارهابيةالتي تنشر نشاطاتها وافكارها عبر الانترنت او تعمل على مهاجمة انظمة الشبكات داخل البلد.

3-تفعيل القوانين الخاصة بالجرائم الالكترونية.

4-الافادة من تجارب الدول الاخرى التي سبقتنا في هذا المجال .

5-ادخال الثقافة السيبرانية ضمن مناهج التعليم ولكافة المراحل.

6-تخصيص الموارد المالية والبشرية اللازمة لنشر الوعي باهمية الامن السيبراني.

المصادر :

1- يحي مفرح الزهراني،الابعاد الاستراتيجية والقانونية للحرب السيبرانية السعودية،مجلة البحوث والدراسات ،جامعة نايف للعلوم الامنية ،العدد23، 2017.
2- سمير بارة،الامن السيبراني في الجزائر السياسات والمؤسسات ،المجلة الجزائرية للامن الانساني،العدد الرابع،2017.
3- عادل عبد الحمزة ثجيل،الامن القومي والامن الانساني،دراسة في المفاهيم ،مجلة العلوم السياسية،العدد2016،51.
4- عبد الرحمن عاطف ابوزيد،الامن السيبراني في الوطن العربي دراسة حالة المملكة العربية السعودية ،المركز العربي للبحوث والدراسات ،بحث منشور بتاريخ 6\4\2020
5- باسم علي خريسان ،الامن السيبراني في العراق قراءة في مؤشر الامن السيبراني العالمي 2020،مركز البيان للدراسات والتخطيط ،2021.
6- ايهاب خليفة،القوة الالكترونية كيف يمكن ان تدير الدول شؤونها في عصر الانترنت ،مطبعة العربي،القاهرة،2017.
7- تغريد معين حسن المشهدي،الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة،مجلة البحوث الجغرافية ،العدد20.
8- جانكارلوأ.بارليتا،ووليام أ.بارليتاوفيتالي تسيجيشكو ،النزاع السيبراني والاستقرار الجيوسيبراني،البحث عن السلام السيبراني،الاتحاد الدولي للاتصالات،2011.
9- سمير قلاع الضروس،الامن السيبراني الوطني:قراءة في اهم الاستراتيجيات الامنية والتقنية لمواجهة الجريمة الالكترونية في الجزائر،مجلة الرواق للدراسات الاجتماعية والانسانية،المجلد8،العدد2 ، 2022.
10- استراتيجية الامن السيبراني العراقي،مستشارية الامن الوطني،امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات