وزاره التعليم العالي والبحث العلمي

جامعة بابل

كلية الإدارة والاقتصاد

قسم العلوم المالية والمصرفية

العنوان: الأمن السيبراني في العراق

بحث مقدم إلى :

مجلس قسم العلوم المالية والمصرفية / كلية الإدارة والاقتصاد هو

جزء من متطلبات نيل شهادة البكالوريوس في قسم العلوم المالية

إشراف: م.د ظلال محمد رضا شويلية

اعداد

محمد المصطفى جعفر جاسم - لقاء كريم فرحان

1444هـ

2023م

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

وَلَئِنِ اتَّبَعْتَ أَهْوَاءَهُمْ مِنْ بَعْدِ مَا جَاءَكَ مِنَ الْعِلْمِ إِنَّكَ إِذًا لَمِنَ الظَّالِمِينَ"

صدق الله العلي العظيم (البقرة ١٤٥)

الإهداء

إلى أبي العطوف.... قدوتي، ومثلي الأعلى في الحياة، فهو من علَّمني كيف أعيش بكرامة وشموخ.

إلى أمي الحنونة..... لا أجد كلمات يمكن أن تمنحها حقها، فهي ملحمة الحب وفرحة العمر، ومثال التفاني والعطاء.

الشكر والتقدير

من لا يشكر الناس لا يشكر الله، وأنت تستحق أندى عبارات الشكر والعرفان فلولا الله ثم أنت لما حققت ما أريد، فقد كنت الداعم الأول، والمحفز الأكبر، والصديق الذي لا يغيره الزمان "ابي"

يعجز الشعر والنثر والكلام كله في وصف فضلك، وذكر شكرك، وتقدير فعلك، فلك كل الثناء وجزيل الشكر، وصادق العرفان على كل ما فعلت وتفعل أمي"

إن قلت شكراً فشكري لن يوفيكم حقّكم، حقاً سعيتم فكان السّعي مشكوراً، وإن جفّ حبري عن التّعبير يكتبكم قلب به صفاء الحبّ تعبيراً إلى مشرفة البحث" الدكتورة ظلال محمد رضا شويلية"

قائمه المحتويات

المقدمة

لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات اللامتماثلية أو اللاتناظرية العابرة للحدود التي لا تعترف بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية.

ومع إنفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن ٢١ وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي وكذلك الدولي لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني " eyber security" كبعد جديد ضمن أجندة حقل الدراسات الأمنية وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال. وأصبح الأمن السيبراني مطلبا ضروريا لكل الدول دون إستثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والإختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكل عام، ويعمل مختصر الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات. فالمارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية والهامة أو يعدلون ويحرفون في معلومات مهمة أو حتى يبثوا معلومات غير صحيحة على مواقع مهمة، وذلك عندما يكون الأمن السيبراني ضعيفًا ويحتاج لتقوية بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية، وأمن المعلومات ليس بعيداً عن الأمن السيبراني، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة والاختراق، ويمنع أي شخص غير مصرح له بالوصول إليها من ذلك، ومن هذا ولأهمية هذا الجانب في حياة الدولة وحياة الأفراد جاءت هذه الدراسة ليستفيد منها الجميع.

مشكلة البحث

ان الغرض من هذا البحث هو دراسة دور الأمن السيبراني في القطاع المصرفي وعليه فإن يمكن تحقيق غرض هذا البحث من خلال الإجابة عن التساؤلات الأتية:

١-مالمقصود بالأمن السيبراني وماهي أشكاله؟

٢-ماهي مخاطر حوادث الأمن السيبراني ؟

٣-مامدى فعالية الأمن السيبراني في القطاع المصرفي ؟

اهمية البحث

تكمن اهمية البحث في ضرورة دراسة الأمن السيبراني وذلك نتيجة التطور التكنولوجي المتسارع الحاصل في جميع نواحي الحياة والتعرف على مخاطر الهجمات السيبرانية ومدى تأثيرها على المصارف الالكترونية.

هدف البحث

يسعى في هذا البحث الى دراسة الأمن السيبراني ومخاطرة على المصارف الالكترونية من خلال :

١-توضيح مفهوم الأمن السيبراني ونشأته واشكاله

٢-توضيح اهميه الأمن السيبراني ومخاطر حوادث الأمن السيبراني.

٣-التعرف على دور الأمن السيبراني في القطاع المصرفي الالكتروني

المبحث الاول

١,١. مفهوم الأمن السيبراني

كلمة سايبر Cyberمشتقة من Cybernetic وأصلها يوناني وتعني التوجيه والسيطرة، وعرفها Norbert Wienerفي عام 1984م "الدراسة العلمية للسيطرة على الأحياء والآلات وآلية التواصل بينها "تختلف استخدامات وأشكال السيطرة على الفضاء السيبراني أو السيادة السيبرانية Sovereignty من دولة إلى أخرى؛ تبعًا لأولويات هذه الدول، فمنها الأمني والسياسي والاستخباراتي والمدني والمهني أو قد يكون معلوماتي بحت، ويتشكل كيان الفضاء السيبراني بشكلٍ عام بوجود ثلاثة مركبات أساسية تضم الأدوات التقنية المستخدمةTechnology، الإجراءات Processes، والعامل البشري من مبرمجين ومستخدمين **People**. كما عرفت هيئة الاتصالات وتقنية المعلومات الأمن السيبراني بنفس تعريف الهيئة الوطنية للأمن السيبراني: "هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة (عتاد) وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك".(**سامي عبد الله الشعلان -٢٠١٨**)

الأمن السيبراني هو مجموع الأدوات والسياسات ومفاهيم الأمن الافتراضي يشمل مفاهيم الأمن وضوابطه وإدارته للمخاطر وآليات الضمان التكنولوجي التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين.(**سيف الهرمزي -٢٠١٦-١٩٥**).

الأمن السيبراني (Cybersecurity): يُطلق عليه أيضاً "أمن المعلومات" و"أمن الحاسوب"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

يعرفه إدوارد أموروسو (Edward Amoroso) صاحب كتاب "الأمن السيبراني" الذي صدر عام 2007 بأنه مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها وتوفير الاتصالات المشفرة .(**مايكل دانيال -٢٠١٧**).

٢,١.نشاة الأمن السيبراني

أن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر -عصر الثورة الصناعية الرابعة -حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير علي ما تمتلكه من معلومات ، لكن العديد من المعلومات والأنظمة والبني التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية)هاكرز (تعطل خدماتها وتدمر ممتلكاتها ، وتختلف هجمات الهاكرز من جهة لأخرى ومن مكان لآخر ومن زمن الى لآخر مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت .وهذا يؤكد على أهمية الأمن السيبراني وذلك للحفاظ على أمن وسلامة الوطن والمواطنين .وقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية . ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرون وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security كبعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

(منى عبد الله السمحان -٢٠٢٢-٤).

وقد نشأ مفهوم الأمن السبراني في عام ١٩٧٢إذ أنه كان مجرد فكرة نظرية في ذلك الوقت، واستمرت النقاشات والتحليلات خلال فترة السبعينيات إلى أن ظهر الأمن السيبراني كمفهوم فعلي قابل للتطبيق. ومع ازدياد الاعتماد على أجهزة الكمبيوتر ونمو الشبكات وانتشارها، ازدادت المناقشات حول أمن الكمبيوتر وأهميته ما بين عام 1972-1974م، وكان من

الضروري تحديد نقاط الضعف، لذا أقرت الحكومات بأهمية الأمن الإلكتروني، وأنّ الوصول غير المصرح به إلى البيانات والأنظمة يمكن أن يكون له عواقب كارثية.(**اثير الخندق – ٢٠٢١**) فقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية والتي حدثت بسبب عاملين أساسيين:.

الأول: استحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة ، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، (Digital)وحفظ المعلومات رقمياً وذلك لتسهيل المهام الموكلة له، وقد تطور ،(CPU) توج بتطوير وحدة المعالجة المركزية ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.

.

الثاني: ظهور الشبكة العنكبوتية(الانترنت) والذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة (Cyber Cold War)أو سباق التسلح السيبراني(Cyber arms race)

(**فارس قرة ـ ٢٠١٩**).

٣,١.<u>اشكال الأمن السبراني</u>

يهدف الأمن السيبراني إلى الدفاع عن أجهزة الكمبيوتر، وكذلك عن الشبكات، والخودام، والأجهزة الخاصة بها من أي محاولة تخريب، ويساعد الأمن السيبراني على حماية المستخدمين من الأنشطة الغير قانونية التي تحدث في عالم الويب المظلم والتي أغلبها ما يكون مهددًا لحياة البشر أو يعرض متصفحه لخطر التعرض للمسائلة القانونية أيضًا، ناهيك عن الناحية الأخلاقية . كما أنّ هناك العديد من أنواع الأمن السيبراني، ومن أهمها ما يأتي:

١-الأمن السحابي:

نظرًا لكون التوجهات الغالبة الآن لمعظم المؤسسات حول العالم هي استخدامها لتكنولوجيا الذكاء الاصطناعي والسحابات التخزينية، أصبح من اللازم تأمين السحابة الرقمية بسبب احتوائها على كمية بيانات هائلة لهذه المؤسسات.

وتقدم مجموعة من الشركات المتخصصة في هذا المجال خدمات لحل تلك الأزمة، مثل Google Cloud وMicrosoft Azure. **(محمد ابراهيم -٢٠٢٠)**

٢- أمن التطبيقات:

تطبيقات الويب مثل أي شيء آخر متصل مباشرة بشبكات الإنترنت، وبالتالي فمن المنطقي أنها تكون مهددة بالهجمات على أمنها السيبراني، وهذا النوع من الأمن السيبراني يساعد الشركات والمؤسسات باكتشاف البيانات الحساسة التي يجب حمايتها من الهجمات المتوقعة، من خلال برامج مضادات الفيروسات، وجدران الحماية، وعمليات تشفير المعلومات.(**وائل جمعة - ٢٠٢١)**

٣- أمن إنترنت الأشياء:

رغم أن استخدام أجهزة إنترنت الأشياء (مثل الأجهزة الذكية وأدوات الذكاء الاصطناعي والمستشعرات الحساسة عبر شبكة عالمية واحدة) يوفر العديد من الفوائد الإنتاجية، إلا أنه يعرض المؤسسات للتهديدات الإلكترونية، يقوم أمن إنترنت الأشياء بحمايتها من خلال اكتشاف الأجهزة المتصلة وتصنيفها حسب دورها التشغيلي بالإضافة لمدى الصلاحية الممنوحة للوصول إلى قاعدة البيانات، وعند استشعار أي حركة غير مألوفة، يقوم بالتحكم في أنشطة الشبكة ومراقبة أي عملية استغلال لهذه الأجهزة وقت التشغيل والتعامل معها. (**مها دحام - ٢٠٢١**)

٤- أمن المستخدم النهائي:

أمان النقاط النهائية تكون عبارة عن مجموعة من الممارسات التقنية تُستخدم في حماية أجهزة المستخدمين النهائيين من الهجمات السيبرانية التي يكون مصدرها البرامج الضارة والغير مرغوب فيها، مثل أجهزة الحاسوب المكتبي والمحمول، والهواتف المحمولة، التي يستخدمها الموظفون في الولوج بشبكات الشركة والوصول إلى الموارد المتعددة، لذلك تسعى المؤسسات

إلى حماية هذه الأجهزة بهدف منع أي محاولة خارجية بالوصول إلى الشبكات وقواعد البيانات المخزنة على خوادم الشركة.(**محمد ابراهيم - ٢٠٢٠**)

٥- أمن البنية التحتية:

يتم تعريف أمان البنية التحتية للمؤسسات بأنه إجراء أمني يقوم على أساس حماية البنية التحتية الحيوية للنظام والحد من نقاط الضعف في هذه الأنظمة من فساد وتخريب وإرهاب، مثل اتصالات الشبكة او مركز البيانات أو الخادم أو مركز تكنولوجيا المعلومات، ويتم وضع خطة طوارئ في حالة استهداف الأنظمة لدى الشركة من قبل مجرمي الإنترنت، (**وائل جمعة - ٢٠٢١**)

٦-الأمن التشغيلي

يهتم الأمن التشغيلي (Operational security) بالمحافظة على العمليات والقرارت التي تُتخذ بشأن معالجة أصول البيانات الإلكترونية وحمايتها، فيراجع هذا النوع من الأمن مختلف الأذونات التي يمتلكها المستخدمون للوصول إلى الشبكة، كما ويحدد أين ومتى تُخزّن هذه البيانات، أو متى يتم مشاركتها مع الآخرين.(**مها دحام - ٢٠٢١**)

٧- أمن الشبكة

يهدف أمن الشبكة (بالإنجليزية: Network security) إلى حماية شبكة الكمبيوتر من أي هجمة تحاول اختراقه سواء كانت هذه الهجمات من داخل هذه الشبكة أو من خارجها.

بحيث يُستخدم هذا النوع من الأمان العديد من التقنيات الحديثة والبروتوكولات التي تساعده على إتمام هذه المهمة.(**مها دحام - ٢٠٢١**).

٨-الأمان المالي:

يظن البعض أن الأمن السيبراني وأمن البيانات غير مرتبطين بالدورة المحاسبية، ولكن بسبب تهديدات القرصنة على البيانات المالية الخاصة بالشركة والتي يمكن أن تشتمل على أخطاء والخرق الغير مقصود للبيانات، تم إنشاء نظام الأمان المالي وإعطاء حلولًا مبتكرة في حالة تم الهجوم على قواعد البيانات من قبل مجرمي الإنترنت، وحماية البيانات من التهديدات

والانتهاكات المالية التي تهدد سبل العيش ونمو الأعمال والعلاقات مع العملاء وغير ذلك(**محمد ابراهيم -٢٠٢٠)**

٤,١. سياسية الأمن السبراني

استراتيجية الامن السيبراني هي نهج موثق تجاه مختلف جوانب الفضاء السيبراني cyberspace.يتم تطويرها في الغالب لتلبية احتياجات الأمن السيبراني للدول والمؤسسات من خلال معالجة كيفية حماية البيانات والشبكات والأنظمة التقنية والمستخدمين. عادة ما تغطي الاستراتيجية الفعالة جميع نقاط الهجوم المحتملة التي يمكن أن تستهدفها الأطراف المهاجمة. يحتل الأمن السيبراني مركز الصدارة في معظم الاستراتيجيات الإلكترونية لأن التهديدات الإلكترونية أصبحت أكثر تقدمًا وخطورة بسبب تقدم أدوات وتقنيات الاستغلال exploit toolsالمتاحة للجميع. بسبب هذه التهديدات ، ننصح المؤسسات بتطوير استراتيجيات تضمن حماية البنية التحتية الإلكترونية الخاصة بها من المخاطر والتهديدات المختلفة. **(حسن هادي لذيذ -٢٠٢٠-٧)** والهدف من هذه الاستراتيجية هو توفير خارطة طريق متماسكة ومبادرات وآليات لتنفيذ و لتحقيق الرؤية الوطنية بشأن الأمن السيبراني. تتألف استراتيجية الأمن السيبراني هي استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية البلد في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به. استراتيجية الأمن السيبراني الوطنية من عدة استراتيجيات قصيرة ومتوسطة وطويلة الأمد تغطي جميع الأوليات الوطنية، وتعالج التعرض الوطني للمخاطر السيبرانية. هنالك تهديدات سيبرانية رئيسية في جميع أنحاء العالم التي تضر بالمصلحة الوطنية. مثل, الجريمة الإلكترونية،الإرهاب الإليكتروني ،الصراع السبراني .التجسس السيبراني ،اساءة معاملة الأطفال واستغلالهم عبر الإنترنت.(**حسن محمد الحسين ، ٢٠١٨ ، ٣٢).** أن لهذه التهديدات قدرة كبيرة على الإضرار بسلامة الأمة، وتعطل عمليات البنية التحتية الحيوية للمعلومات، وتقويضها والعمليات الحكومية، والأمن القومي.

تقوم استراتيجية الامن السيبراني الوطني بتحديد وتنسيق وتوجه البلد في تنفيذ السياسة الوطنية للأمن السيبراني واخذ تدابير متماسكة وإجراءات مضادة ضد التهديدات السيبرانية من أجل تامين وحماية الفضاء الإلكتروني الوطني.(**د. علي زياد العلي ، د. علي حسين حميد، ٢٠٢١ ، ٢٠٦)**

المبحث الثاني

٢.١. أهمية الأمن السيبراني

يعتبر الامن السيبراني الركيزة الاساسية للمجتمع بحيث لا يمكن تصور نمو اي نشاط بعيدا عن تحققه سواء كان ذلك على المستوى التقني ام على المستوى القانوني ، وقد تحول الامن مع بروز مجتمع المعلومات والفضاء السيبراني الى واحد من قطاع الخدمات التي تشكل قيمة مضافة ودعامة اساسية للأنشطة الحكومات والافراد على السواء. الا ان الوجوه المتعددة لاستخدامات القضاء السيبراني ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة الى الافراد والمؤسسات بل تتعداها الى تعريض سلامة الدول والحكومات تزيد مهمة القائمين على الموضوع تعقيدا وصعوبة وتستدعي مقاربة شاملة ومتكاملة لجميع التحديات . ان الموضوع الاهم في الامن السيبراني لا يعني فقط الاجراءات التقنية والادارية المرتبطة بحماية التكنولوجيا والمعلومات فقط بل يتعدى ذلك الى بناء وعي كفوء في ذهن المواطن لكي يتمكن من تحصين نفسه ومجتمعه ويضمن عدم وقوعه ضحية لأي نشاط الكتروني غير شرعي سواء جرائم الكترونية او حتى ارهاب الكتروني ويحصن الفرد من ان يكون اداة تدمير لمجتمعه وثقافته.

بعد ان اصبحت التكنولوجيا واحدة من اساسيات الحياة في مجتمعاتنا ولحداثة التجربة ولكون اغلب الناس المستخدمين للتكنولوجيا لا يفقهون تفاصيل استخدام هذه التكنولوجيا وارتباطاتها

وتأثيراتها والثغرات التي من الممكن ان تخلقها وتنفذ من خلالها لأغلب تفاصيل حياة الناس .. برزت مشاكل خطيرة تهدد الامن الشخصي للناس وبالتالي تشكل خطرا كبيرا على الامن الثقافي ومنظومة الامن الوطني لكون الانسان هو جوهر المنظومة الامنية للبلد. ونظرا لعدم الدراية وغياب الخبرات البسيطة في كيفية استخدام التكنولوجيا الحديثة بشكل امن اصبح الانسان معرضا لمخاطر الكترونية تتعلق بخصوصيته واعماله وجعلته يصبح ضحية لأنواع مختلفة من الهجمات والجرائم الالكترونية على يد مجاميع اجرامية الكترونية اتخذت من الفضاء السيبراني منصة للقيام بأعمالها اللامشروعة. ومثلما كان للجريمة التقليدية مجاميعها وعصاباتها فقد نشأت مجاميع اجرامية وعصابات الكترونية متخصصة بمختلف الجرائم ذات الطبيعة الالكترونية تنوعت بين الجريمة البسيطة المفردة والجريمة الالكترونية المنظمة. تُعد الجرائم الالكترونية من أحد المشاكل العالمية التي تهدد العالم الالكتروني فهي تشكل خطراً على أمن الأفراد وخطراً أكبر على الشركات العالمية الكبرى والمصارف والأنظمة الحكومية. من وجهة نظر الحوسبة، يقابل الأمن الالكتروني اجهزة الأمن والحراسة التي تستعمل في الشركات. حيث يستخدم الأمن الالكتروني لحماية مراكز بيانات والأنظمة المؤتمتة للشركات والمنظمات من الدخول الغير مصرح به. ولقد صممت أنظمة حماية المعلومات للحفاظ على الخصوصية والسلامة توافر البيانات وهي فرع من فروع الأمن الالكتروني. كما يمكن أن يساعد استخدام الأمن الالكتروني على منع الهجمات الالكترونية واختراق البيانات و انتحال الشخصية .**(د. علي زياد العلي ، د. علي حسين حميد ، ٢٠٢١ ، ٢٠٤).**

هناك اهمية لأنشاء وجود درع وطني امني الكتروني تشترك به الاجهزة الامنية للدولة من خلال متابعتها لقضايا الجريمة الالكترونية من جهة، والمواطن بصفته محتوى العمل الامني وكذلك كونه قد يقع ضحية لجرائم الكترونية النزعة من حيث الاحتيال والابتزاز من جهة اخرى، وهذ ياتي باتجاهين الاول يتضمن ضرورة وجود رقابة امنية على الاجهزة الالكترونية واستيرادها وكذلك وجود سيطرة ومراقبة للبرامج والمواقع التي من الممكن ان يصبح المواطن ضحية لها سواء نتيجة لعدم دراية او سوء استعمال او لقلة خبرة او حتى لغياب التشريعات والاجراءات والسيطرة الحكومية في هذا المجال بالإضافة الى الحاجة الملحة لرفع الوعي الامني الالكتروني لدى الناس والذي من شأنه أن يرفع مستوى تحصين المجتمع ومنع حدوث الثغرات التي تستغلها مجاميع العصابات الالكترونية ابتداءا من المستوى البسيط للجريمة الالكترونية وصولا الى الارهاب الالكتروني (**صفاء الوائلي ـ ٢٠٢١**).

وتكمن أهمية الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية ، من خلال مفهوم حرب الإنترنت ((netwar والحرب السيبرانية (cyber war) .

وقد كان هناك تاريخ واسع من الاختبارات النظرية والأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني.(**فارس قرة -٢٠١٩**)

وتكمن أهمية الأمن السيبراني فيما يلى :

١-الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها -تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها . (**منى عبد الله السمحان -٢٠٢٠-١٢**)

٢-حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.

٣-استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

٤-استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

٥-توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتي.

٢.٢.مخاطر حوادث الأمن السبراني

خطر الأمن السيبراني هو الضرر المحتمل أو تدمير أصول الأعمال والإيرادات والسمعة. يحدث هذا الضرر من قبل المهاجمين البشريين الذين يحاولون سرقة المال أو المعلومات أو التكنولوجيا. في حين أن هذه الهجمات تحدث في البيئة التقنية، فإنها غالبا ما تمثل خطرا على مؤسستك بأكملها. يجب مواءمة مخاطر الأمان عبر الإنترنت مع إطار عمل قياس المخاطر وتتبعها والتخفيف منها. لا تزال العديد من المؤسسات تتعامل مع مخاطر الأمان عبر الإنترنت على أنها مشكلة تقنية يجب حلها. يؤدي هذا التصور إلى استنتاجات خاطئة لا تخفف من تأثير الأعمال الاستراتيجي للمخاطر.(**Martin Ekuan-2021**).

كما يُعدّ الأمن السيبراني من المجالات المهمة والمستخدمة في حماية المعلومات من الهجمات الإلكترونية ،لكن ومع ذلك فإنّ هناك العديد من مخاطر الأمن السيبرانيّ التي تواجه الأفراد، والشركات، والمنظمات مع زيادة الاعتماد على التكنولوجيا،(**هالة ابو يوسف -٢٠٢١**) وفيما يأتي بعض هذه المخاطر:

- تهديد الاستقرار المالي Threat to financial stability
- البرامج الضارة malware
- سرقة كلمة المرور Password theft
- قطع واعتراض الازدحام Cut and intercept congestion
- هجمات التصيد Phishing attacks
- رفض الخدمة الموزعةDDOS
- هجوم على المواقع Website attack
- هجوم SQL
- الهندسة الاجتماعية Social engineering
- برامج الفدية ransomware
- كريبتوجاكينج cryptojacking
- هجوم ثقب المياه Water hole attack

٣,٢. <u>الفرق بين الأمن السبراني وأمن المعلومات</u>

أمن المعلومات Information Security و الأمن السيبراني Cyber Security هما مفهومان هامان للغاية في مجال التكنولوجيا، وباتا يستخدمان كثيرًا هذه الأيام. لكن الكثير من الناس الذين يستخدمونهما يخلطون بينهما أو يستخدمونهما كأنهما نفس الشيء، لكن هذا غير صحيح. يعمل الامن السيبراني وامن المعلومات على حماية البيانات من الاختراقات والهجمات وأي خطر محتمل الحدوث. وعلى الرغم من أن هنالك تشابهًا كبيرًا بينهما من حيث المفهوم إلا أنهما مختلفان بعض الشيء ففي الوقت الذي يعمل أحدهما لحماية البيانات في مكانٍ واحد، يقوم الآخر بحماية البيانات بشكلٍ عام.

<u>الامن السيبراني:</u>

هو الأمن الذي يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية وخاصة الإنترنت، حيث يعمل مختصو الامن السيبراني على حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكلٍ عام. كما ويحاول مختصو الأمن السيبراني ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات بالوصول إليها.

(**الدكتور فارس محمد العمارات ، ابراهيم محمد الحمامصة ، ٢٠٢٢ ، ٣)**

امن المعلومات:

يهتم امن المعلومات بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه وليس حماية الحاسب كله(**عبد السلام بن حسن -٢٠٢٠)**

أمن المعلومات هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والاطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخليّة والخارجيّة. (**شهيرة دعدوع -٢٠١٦)**

امن المعلومات يهتم بحماية البيانات المرفقة أصلا على المنصات الالكترونية، والأمن السيبراني يهتم في أن لا تخترق هذا المعلومات ولا تستخدم أصلا من قبل الجهة التي تحفظها. أي انه يطبق على المستخدم شروط الخصوصية التي تحددها الشركة ويسمح لأنظمته الالكترونية الوصول الى كافة المعلومات التي يطلبها مدير التطبيق او مالكه ومن الممكن جدا ان تكون معلومات حساسة وخاصة، أما الأمن السيبراني يمنع عمليات الوصول غير الشرعي لهذه المعلومات من قبل جهات غريبة تحاول ذلك حتى وان أرفقت البيانات على حسابك الشخصي، بهدف حمايتك من عمليات الابتزاز.

1. أمن المعلومات Information security يقوم بحفظ كافة بياناتك عندما توافق على شروط استخدام التطبيق الالكتروني, الأمن السيبراني يمنع التطبيق ذاته من التجسس عليك او ابتزازك وتتبعك من خلال اهتماماتك ومتابعاتك على منصات التطبيق.
2. امن المعلومات من الممكن ان يكون عرضة للاختراق عند استخدام أنظمة تجسس واختراق وفيروسات, اما الامن السيبراني يشكل نظاما الكترونيا يحمي الأجهزة نفسها وراوترات الانترنت من استقبال أي نوع من أنواع الفايروسات, ويتم تبليغ المستخدم بها ليقوم بالخطوات المناسبة لحماية بياناته من إمكانية السرقة التي تهدف الى تشكيل قضايا ابتزاز.
3. Information security. امن المعلومات يمكنه تبليغك بمحاولة اختراق الكتروني لأحد منصاتك او مخازن البيانات التي بحوزتك, ولكن Cybersecurity بإمكانه تتبع المخترق الالكتروني ومعرفة هويته الشخصية وتجميع معلومات عنه فيما يضمن بناء لائحة اتهام كاملة للمخترق معترف بها قانونيا.

4. أمن المعلومات تنتهي اعماله اذا أوقف المستخدم تصريح استخدام معلوماته الذي يعطيه في بداية استخدام التطبيق, مثل تحديد الموقع الجغرافي، اما الأمن السيبراني بإمكانه تحديد مكان المستخدم ونشاطه وتفاعله مع البيئة الخارجية عن طريق وصل اكثر من منصة رقمية وبالاستعانة بأكثر من برنامج الكتروني يستخدمهم نفس الشخص.
5. أمن المعلومات من الممكن ان يحمي الصور والبيانات عن الأشخاص المصنفين عامة على مواقع التواصل الاجتماعي لدى المستخدم، والأمن السيبراني يمكنه الوصول الى كافة البيانات وكافة الهويات التي وصلت الى البيانات بطريقة شرعية وغير شرعية.

المبحث الثالث

٣.١. فاعلية الأمن السبراني في القطاع المصرفي العراقي

أحدثت وسائل التواصل الاجتماعي ثورة في العلاقات بين الناس وآفاقا اقتصادية واجتماعية جديدة لجميع الناس دون تمييز، ولم يكن في الحسبان أنها ستغير علاقتنا الاجتماعية، وستؤثر في الاقتصاد، وتشكل مجتمعاتنا وأن تصبح جزءا من أعمال الحكومة الإلكترونية.

ومما لا شك فيه أن وسائل التواصل أحدثت تأثيرات اقتصادية إيجابية وسلبية في الفرد والمؤسسات والاقتصاد، بل المجتمع ككل. فبالنسبة للفرد جعلت الحياة أرحب وأسهل من خلال التواصل مع الآخرين والتعبير عن الرأي، علاوة على زيادة الإنتاجية وتوسيع إمكانية ممارسة الأعمال والتجارة والبيع والشراء بسهولة كبيرة ولكن هذه الإيجابيات لا تخلو من السلبيات مثل هدر الوقت أو الدخول في علاقات غير شرعية أو التنمر وانتهاك خصوصية الآخرين.

أما بالنسبة لمجال الأعمال، فعلى الرغم من عدم وجود إحصاءات دقيقة، فقد أدت وسائل التواصل الاجتماعي إلى ظهور مهن جديدة مرتبطة بها، وتمكنت كثير من المؤسسات التجارية والتعليمية من ترشيد الإنفاق ورفع جودة الخدمات المقدمة من خلال التواصل مع المستفيدين والعملاء بسرعة وسهولة دون تكاليف تذكر، ومن ثم تحقيق إيرادات أكثر نتيجة تحفيز الطلب

وإنشاء عروض جذابة. إضافة إلى ذلك، أصبح لوسائل التواصل الاجتماعي تأثير عميق في التوظيف باستخدام الشبكات الاجتماعية المهنية مثل LinkedIn، فكثير من مديري التوظيف يتخذون قرارات التوظيف بناء على المعلومات الموجودة على وسائل التواصل الاجتماعي، ونسبة كبيرة من أصحاب الأعمال يستخدمون هذه المواقع للبحث عن المرشحين للوظائف. كما أن هناك منتجات يرتبط وجودها بوجود وسائل التواصل الاجتماعي، ومن الهدايا المجانية لبعض المؤسسات والمحال التجارية والمطاعم أنها تحصل على دعاية مجانية من خلال مستخدمي وسائل التواصل وخاصة سناب شات الذين يتباهون بزيارة بعض المطاعم والأسواق ونحوها.

من جانب آخر، فقد أسهمت وسائل التواصل الاجتماعي في دعم النمو الاقتصادي في أوقات الأزمات وخاصة جائحة كورونا الحالية من خلال تسهيل الاستمرار في التواصل وإبرام العقود وكذلك ممارسة الأعمال بجميع أنواعها والتبادل التجاري بين المؤسسات داخل الدولة وخارجها.علاوة على ذلك، فإنها لها تأثيرا كبيرا في المجتمعات، فقد أصبحت كثير من المشكلات والتحديات الاجتماعية والأخلاقية والبيئية والسياسية أكثر وضوحا للناس، ما يعجل بإيجاد حلول لها.(**رشود بن محمد -٢٠٢٢).**

يعتبر المجال الاقتصادي من بين أهم المجالات التي تحظى بالاهتمام عبر مواقع التواصل الاجتماعي خاصة موقع فيسبوك من خلال تداول موضوعات اقتصادية متنوعة تشمل مختلف الأحداث الاقتصادية سواء ارتبط الأمر بارتفاع الأسعار وانهيارها، أو بمستوى المعيشة، أو بقطاع الزراعة و الصناعة، حيث أن استغلال التطبيقات المختلفة التي تتيحها مواقع التواصل الاجتماعي في هذا المجال، لا سيما وأنها تتميز بالسرعة في نقل المعلومة والسهولة في الاستخدام، يحدث نقلة نوعية في مجال الإعلام الاقتصادي و في نشر الحدث الاقتصادي بشكل خاص خاصة عبر هذه المواقع. (**ليندة ضيف – ٢٠١٥-٢).**

أكد تقرير وسائل التواصل الاجتماعي في العالم العربي الصادر مؤخرا أن " السوشيال ميديا" وشبكات التواصل الاجتماعي تجاوزت مؤخرا مفاهيم التواصل والاتصال وتبادل الآراء بين الناس لتصبح ادوات قوية يمكن استخدامها من قبل الافراد والمؤسسات والحكومات وتطويعها لخدمة الاقتصاد وتطوير عمليات الاعمال التجارية في مختلف القطاعات.

وقد أكد التقرير الذي أصدرته قمة رواد التواصل الاجتماعي العرب في دبي الشهر الحالي ؛ أن هنالك استخداما وانتشارا متزايدا لشبكات التواصل الاجتماعي في المنطقة العربية، وبشكل

متفاوت بحسب الدولة وما تفضله من هذه الشبكات، مؤكدا ان هذه الشبكات يمكن ان تحدث تأثيرات قوية في نمو الأعمال، في تسويق وتحسين صورة المؤسسات، وفي إنشاء الأعمال الجديدة وريادة الأعمال.واوضح التقرير- عن تأثيرات وسائل التواصل الاجتماعي على الاعمال التجارية والاقتصاد – ان المؤسسات في جميع انحاء المنطقة العربية تبنت وسائل التواصل الاجتماعي في أعمالها بوتيرة متفاوتة، ويمكننا تصنيف بعضها على انها مؤسسات تتبنى التغيير والاخرى بطيئة في تبنيه، وعرف المؤسسات التي تتبنى التغيير بانها تلك المؤسسات التي ينظر اليها على انها مؤسسات عصرية وتتحلى بالمبادرة ومتفاعلة ومنفتحة على العالم، وبناءا عليه فهي تستخدم وسائل التواصل الاجتماعي بشكل مكثف في اعمالها لغرض خلق تقارب بينها وبين الجمهور الذي تستهدفه.(**ابراهيم المبضين -٢٠١٥)**

فقد أكدت اغلب الدراسات العراقية أن هنالك دور واضح لشبكة التواصل الاجتماعي في نمو الاعمال التجارية وتسريعها لوتيرة العمل نتيجة لقوة تأثير على المجتمع، وايضاً دورها الفاعل في انشاء اعمال تجارية جديدة وزيادة تسويق المنتجات عبر التواصل السريع مع الجميع بأقل التكاليف، وبما اننا اليوم نعيش ثورة المعلومات والاقتصاد الرقمي وان كل شيء تقريباً أصبح رقمياً، فأن شبكات التواصل الاجتماعي باتت اداة مهمة في تحقيق التقدم الاقتصادي، وهذا واضح من خلال صفحات الدعاية والاعلان والتسويق الالكتروني على هذه الشبكات، اذ لم يعد يقتصر دورها على بث الافكار والاحداث وماشابه، بل هي الان تمثل منصة اقتصادية خدماتية عالمية لتسويق المنتجات من السلع والخدمات بالسرعة الممكنة وبأقل التكاليف وهذا قد يعني نهاية عصر التلفاز والقنوات الفضائية، بل وأكثر من ذلك اصبحت هذه الشبكات هي مشاريع اقتصادية بحد ذاتها تنافس تلك المشاريع الموجودة على أرض الواقع.(**ايهاب علي النواب -٢٠١٨)**

يعتبر العراق من ضمن الدول المستهلكة وليست المنتجة للتطبيقات الإلكترونية فنلاحظ أن العديد من الدول العربية ومنها العراق يستخدم مواقع التواصل الاجتماعي والعديد من التطبيقات الإلكترونية الاخرى فقط ولم يشارك في أنشأ اي تطبيقات تساعد على تطوير وتحسين الاقتصاد العراقي أو العربي أو يسهم في إنتاج اي برامج خاصة بالأمن السبراني في هذا المجال مما جعل العديد من الدول العربية ومنها العراق في مقدمة الدولة المستهلكة حيث أن أغلب الناس في العراق لا يتهم اذا كان التطبيق المستخدم امن ام لا حيث أن أغلب البرامج الحالية التويتر والفيس بوك والعديد من التطبيقات الإلكترونية الأخرى والتي أغلبها تكون غير آمنة.

باتت القرصنة الإلكترونية خطراً يهدد اقتصادات العالم، والتي تتنوع أشكالها بدءاً من اختراق البريد الشخصي أو القرصنة المصرفية لحسابات مالية، وصولاً للتجسس الاقتصادي للحصول على أسرار علمية أو خطط شركات وأنظمة لتطوير منتجاتها. وفي ظل أزمة كورونا التي ضربت العالم خلال عام 2020 زادت الاتهامات لبعض الدول بالتجسس على الشركات العالمية الكبرى، خاصة في الولايات المتحدة وأوروبا والتي تطور لقاحات للوقاية من الفيروس. وكشفت دراسة أميركية في 2019 أن قراصنة المعلوماتية نفذوا حوالي مليوني هجوم في 2018 في العالم أسفرت عن خسائر تزيد عن 45 مليار دولار. وتراجع عدد الهجمات مقارنة مع 2017، لكن الخسائر المالية التي سببتها ارتفعت بـ60%، وتتوقع شركات متخصصة في الأمن السيبراني ارتفاع خسائر القرصنة الإلكترونية بنسبة 15% سنوياً على مدى السنوات الخمس المقبلة. وترى أن الخسائر يمكن أن تصل إلى 6 تريليونات دولار هذا العام و10.5 تريليونات دولار في عام 2025، مقارنة مع 3 تريليونات دولار في عام 2015. **(د. عادل عبد الصادق ، ٢٠٢٠ ، ٣٥)**

كما واعلنت الهيئة المصرفية الأوروبية أن خوادم البريد الإلكتروني التابعة لها تعرضت لاختراق عالمي استهدف خوادم مايكروسوفت لخدمة تبادل الرسائل وأن كل لطبيعته. وجاء في بيان أنه في ختام تحقيق معمق، ذكرت الهيئة ومقرها باريس أن عملية القرصنة كانت "محدودة" وأن سرية أنظمتها وبياناتها "لم تتأثر". وكانت الهيئة من بين المتضررين من عملية القرصنة العالمية التي استهدفت في الأيام الماضية خوادم مايكروسوفت لخدمة تبادل الرسائل. وكانت شركة مايكروسوفت الأميركية قد حذّرت قبلها بأسبوع من أن مجموعة قراصنة باسم "هافنيوم" يستغلون ثغرات أمنية في خوادمها لخدمة تبادل الرسائل لسرقة بيانات مستخدميها المحترفين. وفي الولايات المتحدة تعرضت آلاف الشركات والمدن والمؤسسات المحلية لعملية الاختراق المدعومة بحسب مايكروسوفت من السلطات الصينية. كذلك اتهم تقرير سري للأمم المتحدة كوريا الشمالية باختلاس أكثر من 300 مليون دولار رقمية خلال الأشهر الماضية عبر هجمات إلكترونية، وفق ما نشرته وكالة "فرانس برس" في فبراير/ شباط الماضي. ويشتبه في أن بيونغ يانغ قامت أيضاً بسرقة 81 مليون دولار في 2016 من مصرف بنغلادش المركزي، و60 مليوناً في 2017 من بنك الشرق الأقصى الدولي في تايوان. قامت مجموعة من القراصنة بهجوم غير مسبوق، استولوا فيه على مليار دولار بعد اختراقهم الأنظمة المالية للبنوك بواسطة خطة معدة سلفا، كشفها أحد خبراء شركات الأمن السيبراني لشبكة RT. خطة القراصنة تقوم على إرسال رسائل بريد إلكتروني مع ملفات Word تحتوي على برمجيات

خبيثة يمكن من خلالها الدخول الى الحسابات. ونجح القراصنة في سرقة نحو 100 من المصارف والمؤسسات المالية حول العالم، ومن المرجح أن تكون هذه العملية أكبر عملية سرقة بنوك قد تمت حتى الآن.الغالبية من البنوك التي تم استهدافها كانت في روسيا، إلا أن الهجوم استهدف أيضا مؤسسات مالية في اليابان وهولندا وسويسرا والولايات المتحدة. وقد أشارت شركة "Kaspersky Lab" المتخصصة في أمن الحواسيب، التي يقع مقرها الرئيسي في العاصمة الروسية موسكو، إلى أن هناك 30 دولة و100 مصرف قد تعرضوا لهذه الهجمة التي اسفرت عن خسائر مؤكدة تقدر بحوالي 300 مليون دولار، تطلبت صبرا طويلا من المخترقين الذين قاموا بزرع ملفات تجسس عن بعد ومراقبة منذ عام 2013 ليقوموا بهذه العملية، منوهة إلى احتمال استمرار العملية حتى الآن.و كما كانت عصابة دولية إنترنتية فريدة من نوعها قد تمكّنت بواسطة أجهزة كمبيوتر من إجراء أكثر من 40 ألف عملية سحب، توزّعت على أكثر من 20 بلداً، انتهت بالتهام أكثر من 45 مليون دولار قبل أن تتمكن السلطات الأميركية من القبض على الخلية التي تعمل في نيويورك. وهو الأمر الذي فتح أبواب التساؤل عن مدى ونوعية الحماية التي تتمتع بها الأنظمة الإلكترونية للمصارف العربية، وما إذا كانت تختلف عن تلك التي يتم توفيرها في الولايات المتحدة وأوروبا. كما يوجد قانون في العراق خاصة بنظام الأمن السبراني وهو لضمان وحماية البلد في القضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات ورعاية مجتمع انترنت موثوق به.(**محمد عايش -٢٠١٣**)يصدر مؤشر الأمن

للاتصالات جاءت أمريكا في المركز الاول وبدرجة 100% والسعودية في المركز الثاني بدرجة99.5%.كان ترتيب الدول العربية ضمن مركزها العالمي في الشكل التالي:

الدول	عربيا	عالمياً
السعوديه	1	2
الامارات	2	5
عمان	3	21
مصر	4	32
قطرق	5	27
تونس	6	45
المغرب	7	50
البحرين	8	60
الكويت	9	65
الاردن	10	71
السودان	11	102
جزائر	12	104
لبنان	13	109
ليبيا	14	113
فلسطين	15	122
سوريا	16	126

العراق	17	129
موريتانيا	18	133
الصومال	19	137
جزر القمر	20	175
جيبوتي	21	179

مخطط الامن السيبراني العالمي وتقريره منذ عام 2015 ويعرض المؤشر والتقرير كفاءة دول العالم في الامن السيبراني واجراء مقارنات فيما بينها. وفي نسخة 2021 التي اصدرها الاتحاد العالمي ولم تدرج اليمن في المؤشر.ويلاحظ ان العراق حصل المرتبة 129 عالميا في المؤشر من اصل193دولة، بينما كان في المركز107 في مؤشر عام 2020،مبيناً أن الامن السيبراني وحماية بيانات العراقيين جزء لا يتجزأ من الامن القومي العراقي. وتراجع العراق عربيا،ايضا إذ حصل على المرتبة 17 متقدماً على موريتانيا والصومال، وجزر القمر، وجيبوتي، واليمن،بينما تفوقت عليه بقية الدول العربية بما فيها سوريا، وفلسطين وليبيا، ولبنان، والسودان. وسبب التراجع أن العراق لم يقدم(اجابات عن الاستبيان الذي جمعه فريق المؤشر والذي تضمن بعض المعلومات والبيانات، وهو الامر الذي يطرح عدة اسئلة حول سبب هذا التجاهل للجهات المسؤولة عن هذا ملف الامن السيبراني في العراق). وتشير بعض الدراسات ان هذا التراجع في الملف الامني السيبراني انما يعود الى عدم وجود مؤسسة متخصصة بالأمن السيبراني في العراق(وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها).(**حمزة محمود شمخي -٢٠٢٢).**

كما يوجد قانون خاصة بالأمن السبراني للبنوك العراقية والذي يربط الأمن السيبراني ارتباطا وثيقا بالاقتصاد. فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات. كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات العراقية التي تبحث عن إدارة تكلفة انتاجها بأفضل الشروط الا أن هذا المواقع يطرح مسائل مختلفة تتعلق بحماية مقدم الخدمة أو حماية المستهلك على الانترنت.(**مروة فتحي -٢٠٢١).**

أفادت شبكة العراق الرقمي(DIN) بأن وزارة التعليم العالي والبحث العلمي استحدثت ثلاثة أقسام متخصصة في دراسة الأمن السيبراني. وأوضحت الشبكة، في بيان ، أن "ثلاث جامعات استحدثت أقسام الأمن السيبراني في كلياتها، وهي كل من: جامعة المستنصرية، الجامعة التقنية الشمالية، وجامعة الموصل"، مؤكدةً أنها "المرة الأولى التي يتم استحداث أقسام بهذا التخصص في العراق حيث كانت مناهج الأمن السيبراني تُدرَّس ضمن مناهج كليات علوم الحاسبات وهندستها". وأفادت الشبكة بافتتاح أكاديمية لشركة أمازون AWS المتخصصة بالحوسبة السحابية في أربع جامعات، وأكاديمية أخرى لشركة EC Council المتخصصة في الأمن السيبراني في الجامعة التكنولوجية في العاصمة بغداد اضافةً الى التقنية الشمالية".

يوجد في العراق مؤتمرات حول الأمن السبراني وهو (اتسو العراق) هو أول مؤتمر دولي حول الأمن السبراني أقيم في العراق سنة ٢٠٢١ في بغداد وبمشاركة (٥٢) شركة أجنبية وعربية عاملة في هذا المجال إضافة إلى حضور البعثات الدبلوماسية العاملة في العراق .

ويوجد العديد من المؤتمرات التي أكدت على أهمية الأمن السبراني ومنها:

IEEE S&P – Auckland-1

يقام هذا المؤتمر بشكل سنوي منذ عام 1980 م ، ويعتبر المؤتمر الأصعب من حيث نسبة القبول في النشر وهو أحد المؤتمرات الأربعة الكبار (Big Four)حيث يقام في سان فرانسيسكو ، كاليفورنيا في فندق حياة ريجنسي.

USENIX Security Symposium -2

يقام هذه المؤتمر بشكل سنوي منذ عام 1991م وحتى الآن. يقبل بشكل أساسي الأوراق ذات التطبيق العملي سواء أداة أو نظام وغيرهم، وهو أحد المؤتمرات الأربعة الكبار (Big Four) حيث يقام في أنهايم ، كاليفورنيا.

ACM CCS -٣

يعتبر المؤتمر الأقوى في الأمن السيبراني بالنسبة لمؤتمرات رابطة ACMوالتي تدير جائزة Turing Awardوالتي تلقب أحياناً بجائزة نوبل للكمبيوتر، وهو أحد المؤتمرات الأربعة الكبار ((Big Four)حيث يقام في كوبنهاغن الدنمارك.

NDSS -٤

يشبه كثيراً مؤتمر USENIX Security Symposiumفي شروطه وقد كان سابقاً ضمن رابطة USENIXوهو أيضاً أحد المؤتمرات الأربعة الكبار ((Big Four) حيث يقام في سان دييغو ، كاليفورنيا.

Crypto -5

يعد أهم مؤتمر في علم التشفير، فالمؤتمر مخصص بشكل عام للأوراق المخصصة في التشفير وبروتوكولات التحقق وتأمين الإتصال. حيث يقام في بيتكوين ميامي.

ESORICS -6

يقام هذا المؤتمر بشكل سنوي في أوربا منذ عام ١٩٩٥م ، ويعد المؤتمر الأوربي الأقوى في الأمن السيبراني ويأتي تصنيفه بعد الأربعة الكبار . حيث يقام في لاهاي بهولندا.

ACSAC -7

يعنى هذا المؤتمر بالتطبيقات العملية بشكل رئيسي على طريقة USENIX و NDSS. حيث يقام في اوستن تكساس .

RAID -8

هذا المؤتمر يهتم بشكل أساسي بالأوراق العلمية التي تتحدث عن الهجمات الجديدة أو طرق الدفاع، ولكنه يقبل وينشر الأوراق في المجالات الأخرى في الأمن السيبراني. حيث يقام في برلين .

Blackhat -9

يعتبر المؤتمر الأشهر للعاملين في قطاع تقنية المعلومات وهو يهتم بالمشاكل المستجدة في الأمن السيبراني أو طرق حلها بشكل مختصر Briefings ، كما يشتهر بتقديم دورات مميزة. حيث يقام في سان فرانسيسكو الولايات المتحدة.

DEF CON -10

يقام بشكل سنوي منذ عام 1993م ،أهم ما يميز هذا المؤتمر هو مسابقات التقط العلم التي يقيمها كل سنة CTF حيث يقام في في لاس فيغاس، نيفادا. (**مثنى العقيل -٢٠٢٢).**

الاستنتاج:

١-اكد البحث على أهمية الأمن السبراني للاقتصاد الوطني والعالمي ووضح اهم الفرق بين أمن المعلومات والأمن السيبراني.

٢- أكد على ضرورة الاهتمام بمتطلبات حماية الأنظمة الإلكترونية وخاصة بالنسبة للمصارف لحمايتها من الاختلاس والقرصنة .

٣- تشجيع بحوث ودراسات الأمن السيبراني في أطروحات الماجستير والدكتوراه.

٤- تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني .

5- وضح اهم المشاكل التي تواجه الاقتصاد ومنها القرصنة والتي تسبب خسائر كبيرة في القطاع المصرفي مثال المصرف التجاري الالكتروني

6- التأكيد على أهمية الوسائل الاجتماعية في تحسين وتطوير الاقتصاد بالنسبة للعديد من الدول ومنها العراق اذا لها دور كبير في تنمية الاقتصاد من حيث سهولة وسرعة العمل ليس فقط للأشخاص وانما الشركات أيضا.

7- أكدت على أهمية تشجيع مؤسسات المجتمع المدني والتأكيد على دورها الفعال في التعامل مع الاستخدام غير الأمن لتكنولوجيا المعلومات، وذلك من خلال الأنشطة العلمية ونشر ثقافة الاستخدام الأمن لشبكة الانترنت والتطبيقات الرقمية الحديثة.

8-كما بينت أن يجب على الدولة اجراء مزيد من الدراسات العلمية حول قضية أمن المعلومات بمختلف المؤسسات ، ومجال التعليم بشكل خاص.

9- كما بينت على أن هناك مجموعة من الجامعات التي افتتحت قسم خاص بالأمن السيبراني داخلها من أجل الاهتمام بهذا القسم وتطويره .جامعة المستنصرية، الجامعة التقنية الشمالية، وجامعة الموصل.

المصادر

1. الدكتور فارس محمد العمارات ، ابراهيم محمد الحمامصة ، الأمن السيبراني المفهوم وتحديات العصر ، ٢٠٢٢ ، دار الخليج للنشر والتوزيع، الأردن.
2. د. عادل عبد الصادق ، الاقتصاد الرقمي وتحديات السياسة السيبراني ، ٢٠٢٠ ، المركز العربي للأبحاث الفضاء الإلكتروني.
3. حسن محمد الحسين ، اساسيات الأمن السيبراني ، ٢٠١٨ ، دار الكتاب العربي ، القاهرة مصر.

4. د. علي زياد العلي ، د. علي حسين حميد ،تكتيكات الحروب الحديثة: الأمن السيبراني والحروب المعززة والهجينة، ٢٠٢١ ، دار الكتب العلمية ، بيروت لبنان.
5. حسن الفني ،تعريف الأمن السيبراني ،٢٠٢٢.
6. سامي عبد الله الشعلان ،مفهوم الأمن السيبراني ،٢٠٢٠.
7. مايكل دانيال ، الأمن السيبراني ،٢٠١٧.
8. مني عبد الله السمعان ،متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية ،٢٠٢٠.
9. اثير الخندق ،ما هو الأمن السيبراني ؟ ومتى نشأ ،٢٠٢١.
10. مهام دحام ، ما هي أنواع الأمن السيبراني وما أبرز التحديات التي يواجهها ،٢٠٢١.
11. هاله ابو يوسف ، سجى الدقامسة – مخاطر الأمن السيبراني،٢٠٢١.
12. حسن هادي لذيذ ، أساسيات استراتيجية الأمن السيبراني العقوبة ، ٢٠٢٠.
13. فارس قره ، الأمن السيبراني ،٢٠١٩.
14. عبد السلام بن حسن ابراهيم ، الفرق بين أمن المعلومات والأمن السيبراني ، ٢٠٢٠.
15. مثنى العقيل ، اهم عشر مؤتمرات في الأمن السيبراني ،٢٠٢٠.
16. مروة فتحي السيد البغدادي، اقتصاديات الأمن السيبراني في القطاع المصرفي،٢٠٢١.
17. حمزة محمود شمخي ، مؤتمر الامن السيبراني وموقع العراق فيه ،٢٠٢٢
18. ديف لي ، الحكومة الأمريكية واختراق النظام العالمي المصرفي ،٢٠١٧.
19. محمد عايش ، اختراق الالكتروني تهدد أموال البنوك الخليجية، ٢٠١٣
20. ابراهيم المبيضين، دراسات شبكات السوشيال ميديا تطور الاقتصاد والاعمال التجارية، ٢٠١٥.
21. ليندا ضيف، الحدث الاقتصادي عبر مواقع التواصل الاجتماعي ودراسة تحليلية لعينة من صفحات الفيسبوك ،٢٠١٥.
22. حسن جمعة الرئيسي ، الأزمة الاقتصادية ووسائل التواصل الاجتماعي ، ٢٠١٩.
23. رشود بن محمد الخريف ، اقتصاديات وسائل التواصل الاجتماعي ،٢٠٢٢.
24. شهيرة دعدوع ، مفهوم أمن المعلومات ،٢٠١٦.

25. ايهاب علي النواب ،شبكات التواصل الاجتماعي وتطوير الاقتصاد ،٢٠١٩.
26. سيف الهمزري، مفهوم الأمن السيبراني ، ٢٠١٦.
27. محمد ابراهيم ، أنواع الأمن السيبراني ، ٢٠٢٠.
28. وائل جمعة ، أنواع الأمن السيبراني ، ٢٠٢١.
29. صفاء الوائلي ، أهمية الأمن السيبراني ، ٢٠٢١.

الروابط الالكترونية

1. https://sotor.com/%D9%85%D8%A7_%D9%87%D9%8A_%D8%A3%D9%86%D9%88%D8%A7%D8%B9_%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%9F_%D9%88%D9%85%D8%A7_%D8%A3%D8%A8%D8%B1%D8%B2_%D8%A7%D9%84%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA_%D8%A7%D9%84%D8%AA%D9%8A_%D9%8A%D9%88%D8%A7%D8%AC%D9%87%D9%87%D8%A7%D8%9F
2. https://cyberone.co/%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/
3. https://aws.amazon.com/ar/what-is/cybersecurity/
4. https://www.e3melbusiness.com/blog/cyber-security
5. https://attaa.sa/questions/view/744
6. https://rattibha.com/thread/1328799226139185152
7. https://www.alaraby.co.uk/economy/%D8%A7%D9%84%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%87%D9%84-%D8%AA%D8%B9%D9%84%D9%85-%D9%82%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%AE%D8%B3%D8%A7%D8%A6%D8%B1-%D8%A7%D9%84%D8%AA%D9%8A-%D8%AA%D9%83%D8%A8%D9%91%D8%AF%D9%87%D8%A7-

%D9%84%D9%84%D8%B9%D8%A7%D9%84%D9%85%D8%9F
8. https://baghdad-times.net/%D8%B9%D8%A7%D8%AC%D9%84-%D9%87%D8%A7%D9%83%D8%B1%D8%B2-%D9%8A%D8%AE%D8%AA%D8%B1%D9%82-%D9%85%D9%88%D9%82%D8%B9-%D9%85%D8%B5%D8%B1%D9%81-%D8%A7%D9%84%D8%B1%D8%A7%D9%81%D8%AF%D9%8A%D9%86-%D8%A7%D9%84/