الأمن السيبراني ومكافحة الجرائم الإلكترونية

وداد حقي إسماعيل أ.م.د محمد علي فدعم

جامعة الأنبار – كلية الآداب – قسم علم الاجتماع

wid23a6008@uoanbar.edu.iq

art.fadam61@uoanbar.edu.iq

الملخص

يمثل الأمن السيبراني ومكافحة الجرائم الإلكترونية أولوية أساسية في عالم متصل تكنولوجيا. مع تزايد التهديدات مثل الاختراقات والاحتيالات، يتطلب الأمر استراتيجيات فعالة لحماية البيانات والمعلومات الحساسة. تتعاون الحكومات والشركات لتبني تقنيات متقدمة وتوعية المجتمع حول أهمية الأمن الرقمي. يعد الاستثمار في التدريب والتطوير أمرًا ضروريًا لمواجهة هذه التحديات المتطورة. من خلال جهود جماعية، يمكن بناء بيئة رقمية أكثر أمانًا وموثوقية.

الكلمات المفتاحية: (الأمن السيبراني، الجرائم الإلكترونية، الحماية، التوعية، التكنولوجيا).

Cybersecurity and Cybercrime Combating

Widad Haqqi Ismail Assoc. Prof. Dr. Mohamed Ali Fadam

Anbar University – College of Arts – Department of Sociology

wid23a6008@uoanbar.edu.iq

art.fadam61@uoanbar.edu.iq

Abstract

Cybersecurity and combating cybercrime are a key priority in a technologically connected world. With the increase in threats such as hacks and frauds, effective strategies are required to protect sensitive data and information. Governments and businesses are collaborating to adopt advanced technologies and educate society about the importance of digital security. Investing in training and development is essential to address these evolving challenges. Through collective efforts, a safer and more reliable digital environment can be built.

Keywords: (Cybersecurity, cybercrime, protection, awareness, technology).

المطلب الاول: عناصر الدراسة

أولاً: مشكلة الدراسة

تتمثل مشكلة الدراسة في ضعف استراتيجيات الأمن السيبراني المعتمدة من قبل الجهات الأمنية في العراق، مما يؤدي إلى زيادة الجرائم الإلكترونية. تعاني هذه الجهات من قلة التدريب والموارد اللازمة للتصدي لهذه الأنواع من الجرائم، بالإضافة إلى نقص الوعي حول المخاطر المحتملة.

ثانياً: أهمية الدراسة

تكمن اهمية الدراسة للأمن السيبراني مع تزايد الاعتماد الاشخاص والدول والشركات حول العالم على التكنولوجيا ووسائل الاتصال الحديثة، واصبح الامن السيبراني عنصراً اساسياً في عالمنا الرقمي الحديث، نتيجة هذا الاعتماد المتزايد على التكنولوجيا افرزت البيئة الرقمية الجرائم الإلكترونية المعقدة، وان اندماج الافراد في العالم الافتراضي، و الارتفاع الشديد في خسائر الجرائم الإلكترونية مقارنة بالخسائر فى الجرائم التقليدية تدعو الى تعزيز اهمية الامن السيبراني لمواجهة ومكافحة الجريمة الإلكترونية المستحدثة وحماية البيانات والمعلومات الحساسة وتعزيز الثقة في البيئة الرقمية، فالأمن السيبراني هو ضرورة حتمية لحماية العالم الافتراضي والعالم الواقعي، اما على المستوى المحلى لوحظ في السنوات الأخيرة في العراق تزايدًا ملحوظًا في الجرائم الإلكترونية بسبب انتشار التكنولوجيا، وزيادة الاعتماد على الإنترنت، وضعف التشريعات والأطر التقنية و تتنوع هذه الجرائم بين اختراق الحسابات، والارهاب السيبراني، وانتحال الشخصية والابتزاز الإلكتروني، والاحتيال المالي، والتشهير، ونشر الأخبار الكاذبة والتزوير والاتجار بالبشر وغيرها.

ثالثاً: الاهداف

رغم الايجابيات التي وفرتها الثورة التكنولوجية إلا ان تلك الثورة رافقها تغير في عالم الجريمة، حيث ظهرت الجريمة الإلكترونية من رحم العالم الافتراضي، فهي جريمة مرتبطة بتقنيه المعلومات والحواسيب. إذ تمثلت أهداف الدراسة بالآتي:

١ . ماهية الامن السيبراني والمفاهيم المرتبطة به؟

٢. ماهي الجريمة الإلكترونية وما هي خصائصها؟

٣ . الوقوف على أكثر الجرائم الإلكترونية انتشاراً و آليات مكافحتها؟

المطلب الثاني: المفاهيم المتعلقة بالدراسة

١. الامن السيبراني من المفاهيم المعقدة الذي يتكون من كلمتين هما الامن وسايبر:

أ . الأمن لغة: هو نقيض الخوف. والفعل الثلاثي أمِن أي حقق الأمان بمعنى السلامة. والاطمئنان. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً: أي اطمئنان النفس وسكون الروح وزوال الخوف والقلق، ويقال: أَمِنَ من الشر والاذى، أي سَلِمَ منه وانه يشير إلى غياب ما يُهدد القيم النادرة(١).

اما قاموس الامن الدولي فقد عرف الأمن ضمناً عدم وجود تهديد بمعنى أن يكون المرء آمناً وإما لا يكون، وإما أن تكون هناك تهديدات وإما لا تكون؛ ومن ثم يمكن أن يتوافر للمرء درجات مختلفة من الأمن، ووقاية من التهديد أكبر(٢).

قال ابن منظور: "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال آمن به قوم وكذب به قوم"(٣).

اما سايبر جاءت في قاموس المورد بمعنى علم الضبط(٤) وجاءت في قاموس المصطلحات العسكرية الامريكية هو اي فعل بقصد يستخدم عن طريق شبكات الانترنيت للسيطرة او للتعديل على البرامج الكترونية اخرى(٥). وجاء في قاموس مصطلحات الامن المعلوماتي هو كل هجوم عبر الفضاء الالكتروني يهدف الى السيطرة على مواقع الكترونية او بنى محمية الكترونيا لتعطيلها او تعديلها او تدميرها او الاضرار بها او سرقة معلومات ذات اهمية للمؤسسة او الجماعة او الفرد(٦).

. اما الامن السيبراني اصطلاحاً: انه عباره عن مجموعة من الانظمة التي تقوم بمهمة تجميع ادوات ووسائل واجراءات امنية وتدريب لإدارة المخاطر والاستراتيجيات الامنية التي يمكن استخدامها لحماية المجتمع السيبراني(٧).

ثانياً . الجريمة

الجريمة تعرف لغويا بمعنى الجناية وبمعنى الذنب، ورد في لسان العرب: "وجرم إليهم وعليهم جريمة وأجرم: جنى جناية"(٨).

وفي تاج العروس، والجرم بالضم الذنب كالجريمة، وقال: والمجرمون في قوله تعالى: {وَكَذَلِكَ نَجْزِي الْمُجْرِمِينَ} الكافرون لأن الذي ذكر من قصتهم التكذيب بآيات الله والاستكبار عنها قاله الزجاج

والذي يلفت النظر، أن لفظة الإجرام وردت في كثير من الآيات الكريمة، وكلها والله أعلم يقصد بها الكافرون أو المشركون ونحوهم من المكذبين والمنافقين. كما نقله صاحب التاج عن الزجاج، كما ورد في قوله تعالى: {سَيُصِيبُ الَّذِينَ أَجْرَمُوا صَغَارٌ عِنْدَ اللَّهِ وَعَذَابٌ شَدِيدٌ بِمَا كَانُوا يَمْكُرُونَ} الأنعام: ١٢[٩].

الجريمة اصطلاحا

عرفها قانون العقوبات: هي كل عمل او تصرف يخالف امرا او نهياً أو جبته قاعده من القواعد التي تنظم سلوك الانسان في الجماعة، ويباشر في وسط اجتماعي معين[١٠]. وكذلك تعرف انها اشباع لغريزة انسانية بطرق شاذه لا يسلكه الانسان العادي حين يشبع الغريزة نفسها وذلك لأسباب نفسية انتابت مرتكب الجريمة في لحظة ارتكابها بالذات[١١]. الجريمة في الشريعة الاسلامية : بأنها محظورات شرعية زجر الله عنها بحد او تعزيز، والحظورات هي اما اتيان فعل منهي عنه او ترك فعل مأمور به[١٢] .والجريمة عند جاروفالو هي اعتداء على القيم الاجتماعية الاساسية[١٣].

ثالثاً: الجريمة الإلكترونية

اولاً – يعرف الالكتروني لغة وهو المنسوب إِلَى الالكترون، وهي الة الحاسوب تستند على ماده الالكترون لإجراء ادق العمليات الحسابية وبأقصر وقت ممكن ويسمى أيضاً كمبيوتر وعِلْمُ الالكترونيات يهتم بتركيب الالكترونيات واستخدامها وهم فرع من الفيزياء[١٤].

اما تعريف الجريمة الإلكترونية اصطلاحا من الجانب القانوني على انها مجموعة من الافعال والانشطة والسلوكيات المعاقب عليها قانونيا والتي تربط بين الفعل الاجرامي والثورة التكنولوجية وبمعنى اخر هي النشاط الاجرامي الذي تستخدم في التقنية الإلكترونية الرقمية بصورة مباشرة او غير مباشرة كوسيلة لتنفيذ الفعل الاجرامي المخطط له من قبل الجاني وهي جرائم ذات صلة بعلم المعالجة المنطقية للمعلوماتي، اما من الجانب الفني فهي كل انحراف يستخدم الحاسب الالي او أي جهاز الالكتروني بطريقة غير سليمة لأهداف التخريب او احداث فوضوى قصدية[١٥]، و هي كل سلوك غير قانوني يتم باستخدام الاجهزة الإلكترونية يهدف عنها حصول المجرم على فوائد مادية او معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من اجل السرقة او اتلاف المعلومات او دافع ذاتية مثل زعزعة الامن النفسي[١٦].

رابعاً: المصطلحات ذات صلة بالأمن السيبراني

أ . الحرب السيبرانية: عرفها قاموس الامن الدولي (هي حرب تنشأ من خلال اجهزة الحاسوب وشبكة الانترنيت، وهي حرب تضم الهجمات السيبرانية بهدف الحاق الضرر بمعلومات الاخرين واخرى تكون دفاعية لحماية النظم الخاصة بالمهاجمين وتهدف حرب الانترنيت استغلال معلومات الاخرين، وخداع العدو وتعطيل نظم المعلومات، واطلق عيها العديد من التسميات الاخرى مثل حرب الانترنيت او الحرب القائمة على الشبكات او حرب البريد الالكتروني او الحرب الافتراضية[١٧].

ب . الارهاب السيبراني

الارهاب لغةً: ان كلمة ارهاب مشتقه من الفعل "رهب، يرهب، رهبة" بمعنى اخاف، ورهبة بمعنى اخافة ؟، والرهبة هي الخوف والفرع هو راهب من الله أي خاف من عقابة، وترهبة بمعنى توعده[١٨].

الارهاب السيبراني: بمعنى هجوم متعمد ذو دوافع سياسية او اقتصادية او اجتماعية او ذاتية، ضد انظمة المعلومات والبرامج والبيانات التي تهدد بالعنف او تؤدي للعنف ويشمل المصطلح أي هجوم الكتروني يخيف او يولد الخوف لدى السكان المستهدفين، وغالبا ما يقوم المهاجرون بذلك عن طريق اتلاف البنية التحتية الحيوية او تعطيلها وتستخدم الجماعات الارهابية بشكل متزايد الهجمات السيبرانية للاضرار بمصالح الدولة واحداث خلل في استثرارها وامنها[١٩].

ت – الهجوم السيبراني

وجاء في معجم اللغة العربية المعاصرة هجوم دفاعيّ: تصدٍّ نشيط لتهديدات متوقَّعة- هُجُوم وَحْشيّ وهو عمل يتميز بالقسوة الشديدة أو الشراسة أو الحقد هجوميّ، مُنخرط أو موجَّه للهجوم المُسلَّح هَجْمة، دخول مفاجئ سريع في عنف وقوَّة والهجوم هو حرب ساحقة و شديدة ومدمِّرة[٢٠].

المطلب الثالث: الدراسات السابقة والنظرية المفسرة للدراسة

تعتبر الدراسات السابقة والنظرية المفسرة للدراسة عنصران اساسيان في البحث العلمي، فالدراسات السابقة هي عرض يقدمه الباحث للدراسات او الابحاث التي اجريت في نفس المجال التي يدرسه الباحث.

اولاً: الدراسة العراقية

دراسة الباحثة د. شيماء تركان صالح، الامن الوطني العراقي والتهديدات السيبرانية الارهاب السيبراني نموذجاً) ٢٠٢٣[٢١].

ادى الاعتماد على استخدام شبكات الانترنيت في العراق الى احداث ثوره معلوماتية كبرى وتركت تأثيراتها على جوانب الحياة كافة، وأصبح امن الدولة يواجه تحديات جديدة تمثلت بالتهديدات السيبرانية. فالتطور التكنولوجي الذي شهده العراق في مجال والمعلومات والمعلومات والذي تزامن مع ضعف الامن لدى البنية التحتية الوطنية، ادى الى ان يصبح العراق منكشفا امام التهديدات السيبرانية مختلف اشكالها، واعتمدت مشكلة الدراسة في البحث على اجابه السؤال الذي مفاده (ما المقصود بالسيبرانية والارهاب السيبراني، ومتى انتشرت السيبرانية في العراق ومتى ظهر الارهاب السيبراني في العراق وما هي مظاهرة، وما هو واقع الامن السيبراني في العراق).

. اهمية الدراسة: تأتي من كون الارهاب في العراق اصبح متواجد في التكنولوجيا الرقمية حيث اصبح هناك حربا الكترونية متعددة الفواعل والمساحة والانماط في ان واحد مما جعل من الصعب مواجهتها والسيطرة عليها وهي تشمل التجنيد وجمع الاموال والمتطوعين وجمع المعلومات حول الاهداف العسكرية بهدف تدميرها.

اما اهداف الدراسة فقد جاءت:

أ. ماهي متطلبات استراتيجية مكافحه الارهاب السيبراني في العراق.

ب. ماهي مكامن الخلل في الامن السيبراني العراقي.

ج. متى ظهر الارهاب السيبراني في العراق وما هي مظاهره.

د. وقد استخدمت الباحثة في دراستها منهج المسح الاجتماعي والمنهج الوصفي.

توصلت الدراسة الى بعض النتائج:

أ. ضعف القوانين والتشريعات الحكومية الخاصة بالأمن السيبراني:

ب. عدم وجود قانون ينظم الامن الوطني السيبراني، ويمكن الاشارة الى المخاض العسير الذي يمر به قانون الجرائم الإلكترونية الذي تم مناقشته في مجلس النواب منذ عام ٢٠١١م ولا

يزال مطروحا في مجلس النواب منذ أكثر من عشر سنوات ولم يطبق حتى الان بسبب سوء الصياغة والمبالغة التي وردت فيه.

ج. عدم وجود هيئة مستقله للأمن السيبراني، حيث ان العراق حاول مسايرة بعض الدول في موضوع الامن السيبراني فأنشأ هيئة واحده للأمن السيبراني وهي فريق الاستجابة الريعة للأحداث السيبرانية) ولازال موقعها الالكتروني يتعرض للاختراق وتم اتهامه من قبل وسائل الاعلام بالفساد الاداري.

د. قله إدراك الشركات المحلية في مجال التكنولوجيا المعلومات بحجم المخاطر الامنية المعاصرة و ارتباط منظومة الانترنيت في العراق بدول الخارج وشركات خارجية.

هـ. ضعف المهارات والقدرات المحلية في الامن السيبراني.

ثانياً: دراسات عربية

دراسة الباحث ايمن محمد فارس الدنف: (واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها)، ٢٠١٣[٢٢].

ان امن المعلومات عبارة عن مجموعة من الاجراءات والتدابير الوقائية التي تستخدم للحماية من جرائم الحاسوب والانترنيت وان تهديدات استخدام التقنيات منها سرقة المعلومات او السرقة و شبكات المعلومات والبيانات المتعلقة بالبيانات الشخصية، وكذلك الشركات والمؤسسات، لذلك لابد من اجراء عملية ادارة المخاطر بفعالية.

تأتي مشكلة الدراسة مع تزايد تحديات امن المعلومات في البيئة الرقمية كلما تعمقنا في الحوسبة الحديثة، ومع اتساع نطاق مؤثرات الداخلية والخارجية تصبح التقنيات وحدها عاجزة عن التغلب على المخاطر الامنية التي تحدق بهذه النظم، وضع الباحث تساؤلات للدراسة منها:

١. ما هو واقع ادارة نظم المعلومات في الكليات التقنية بقطاع غزة؟

٢. ماهي سبل تطوير ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزه؟

٣. ما هي سبل تطوير ادارة نظم المعلومات في الكليات التقنية بقطاع غزه؟

أهمية الدراسة: تنبع اهمية هذه الدراسة من كونها تسلط الضوء على اداره امن المعلومات في التعليم العالي تحديدا في الكليات التقنية، أصبح الامن المعلوماتي من القضايا التي نالت اهتمام صناع

القرار والسياسيين والاستراتيجيون على الصعيد المحلي والعالمي، مساعده الجهات المشرفة في الكلية التقنية في التعرف الى واقع اداره نظم المعلومات في الكليات التقنية في محافظة غزة، ورسم صوره واقعية حول واقع الكليات التقنية وامن نظمها وتطوير هذه الاداريات.

هدفت الدراسة الى التعرف على واقع امن نظم المعلومات في الكليات التقنية بقطاع غزة، والكشف عن مهددات امن نظم المعلومات في الكليات التقنية بقطاع غزة، والسعي للتحقق من فعالية اساليب امن المعلومات المستخدمة، و بيان مدى استخدام التعهيد (الاستعانة بالأطراف الخارجية) في الكليات التقينه.

اعتمد الباحث على المنهج الوصفي والمنهج الميداني متبعا خطوات المقابلة المباشرة، وجمع البيانات و**توصل الى بعض النتائج التالية:**

١. العمل على توفير البنى التحتية لنظم المعلومات في الكليات التقنية.

٢. يجب إدراك للكليات التقنية اهمية سياسات امن المعلومات.

٣. لا توجد خطط جاهزة لاستعادة العمل في حالات الطوارئ لدى اغلب الكليات.

٤. تقوم اغلب الكليات بإجراء عملية النسخ الاحتياطي الاعتيادي في حالة الطواري.

ثالثاً: الدراسة الاجنبية

دراسة الباحث علي فايز بعنوان (تهديدات امن المعلومات ضد خدمات الهاتف المحمول) ٢٠٠٩[٢٣].

مشكلة هذه الدراسة تتمحور حول الهجمات الضارة او المهاجمين الالكترونين عند استخدام الاجهزة المحمولة، وتأتي اهمية دراسة الباحث في تحليل الحالات لتوفير بيان قوي للحفاظ على امن المعلومات ومعرفة الاثار والتهديدات المحتملة لهذه المخاطر والمساهمة في البحث عن العيوب في الاجهزة الإلكترونية، واستخدم الباحث المنهج البحث النوعي مع استخدام نمهج دراسة الحالة كاستراتيجية ليتم جمع البيانات من خلال المقابلات العميقة.

إذ تكمن أهمية الدراسة في ان البرامج الخبيثة والتهديدات تشكل خطرا على بيئة الكمبيوتر مثل سرقه المعلومات او تعطيل خادم البريد الالكتروني، حيث ان الاجهزة الحديثة يمكن ان تستغل بيانات

المستخدم مثل السرية وتزيف المعلومات وارسال البرامج الضارة ويمكن استخدام برامج تجسس تؤذي الافراد.

وهدفت الدراسة الى الحصول على فهم أفضل للأمن والى كيفية تحسين خدمات الهاتف ضد التهديدات والهجمات السيبرانية ن وكيف يمكن تطوير خدمات الهاتف المعلوماتية.

إذ اعتمد الباحث على المنهج الاستكشافي بهدف جمع أكبر قدر من المعلومات حول موضوع الدراسة، وكذلك اعتمد على المنهج الوصفي لوصف الانشطة المعقدة واعتمد كذلك على منهج دراسة الحالة ليتم جمع البيانات عن طريق المقابلة والملاحظة والوثائق والسجلات السابقة

توصل الباحث الى بعض النتائج وكان اهمها:

١. تحسين امن التطبيقات والخدمات، يستطيع البرنامج ان يتحسس إذا كان البرنامج غير امن.

٢. القليل من التقنيات التي تواجهه التهديدات التقنية.

المطلب الرابع: نشأه الامن السيبراني

تعود نشأه الامن السيبراني الى القرن العشرين تزامنا مع تطور التكنولوجيا. و ظهر مع بداية الحرب الباردة وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسي ومع تزايد الاعتماد على الانترنيت ظهرت التهديدات والجرائم السيبرانية، وان ظهور الامن السيبراني مر بعده مراحل وهي:

المرحلة الاولى : ظهرت الامن السيبراني لأول مرة في الخمسينات من القرن العشرين واستحداث اجهزة الكمبيوتر لحفظ المعلومات رقميا حيث توجهت هذه الجهود بتطوير وحده المعالجة المركزية (CPU) وذلك لتسهيل جميع المهام حيث تم انشاء اول كمبيوتر في عام ١٩٤٣ وعلى مدى العقود التالية كانت هناك طرق محدودة للأفراد لاستخدام اجهزة الكمبيوتر بطريقة اجرامية او محفوفة بالمخاطر، حيث لم يكن هناك الا القليل من اجهزه الكمبيوتر حول العالم ولم تكن هذه الاجهزة الإلكترونية متاحة لأغلب الافراد، حتى اواخر عقد الاربعينات، وتطورت الكثير نظرية حول الفيروسات، واعتقد جون فون نيومان ان نوعاً ما من الكائنات الحية يمكن ان تصنع وامكانية هذا الكائن من نسخ نفسة مثل الفيروس الحي الطبيعي، وهذا يؤدي الى اتلاف الآلات الرقمية[٢٤].

المرحلة الثانية: شهدت الولادة الحقيقية للأمن السيبراني في السبعينات، حيث بدأت بمشروع يسمى شبكة مشاريع الابحاث المتقدمة فكانت هذه هي شبكة الاتصال التي تم تطويرها من قبل الانترنيت نفسة ففي عام ١٩٧١ توصل رجل يدعى بوب توماس الى ابتكار برنامج مقبول على نطاق واسع باعتبارة اول برنامج على الاطلاق في الكمبيوتر من نوع البرامج الضارة او الخبيثة (MAIWARE) والذي يعرف بحصان طروادة. بدأت وكالة الابحاث المتقدمة (ARPA) في المشاريع المتطورة وهي قسم من وزاره الدفاع الامريكية في تطوير امن الشبكات، وكذلك الابحاث في ستانفورد، وجامعة كاليفورنيا في لوس انجلوس. وفي عام ١٩٧٩، تم القاء القبض على اول مجرم الكتروني والذي يدعى كيفن ميتنك، وكان هذا الهجوم الاول من الهجمات الإلكترونية [٢٥].

المرحلة الثالثة: في الثمانينيات ومع نمو التقنيات والتوسع واعتماد معظم الشبكات على انظمة الاتصال زاد الطلب على طرق حماية وتأمين الشبكات وبذات الحكومات في البحث عن سبل للحد من التهديدات الإلكترونية والهجمات وظهرت الهجمات الإلكترونية وظهرت العديد من مشاكل الانترنيت من ضمنها جريمة ماركوس هيس الماني الجنسية[٢٦].

المرحلة الرابعة: في التسعينات شهد تطورا في صناعة الامن السيبراني، وتم تطوير اول برنامج مضاد للفيروسات من قبل مجرمي الانترنيت، وفي أوائل القرن الحادي والعشرين بدأ القراصنة في شن الهجمات على الانترنيت، فبدأت المنظمات الاجرامية في تمويل الهجمات الإلكترونية الاحترافية بكثافة وبدأت الحكومات في تضيق الخناق على جرائم القرصنة واصدار العقوبات المالية عليهم وكذلك استمرار نمو وتقدم امن التكنولوجيا والمعلومات ولا زالت صناعة الامن السيبراني في النمو، وفي عام ١٩٨٣ ظهرت مصطلحات جديدة لوصف الهجمات الإلكترونية مثل (حصان طروادة)[٢٧].

المطلب الخامس: انواع الامن السيبراني

الامن السيبراني او امن الكمبيوتر وهو وسيلة لحماية البرمجيات او المعلومات الشخصية وهو على عدة انواع منها:

أولاً- أمن الشبكة: هو حماية البنية التحتية للشبكات الاساسية من الوصول (الغير مصرح به)* ومن أغلب الهجمات التي تكون عبر الشبكات الإلكترونية، لذلك تم وضع أنظمة أمنية تعمل كصمام أمان

للشبكة، وتضمن تلك الأنظمة حلول فورية وتحكم كاملٍ في عناصر البيانات والوصول للشبكة، حتى تمنع أي هجمات تحاول سرقة أو اتلاف تلك البيانات المخزنة على الخوادم الخاصة بها.

ثانياً- أمن التطبيقات: هي الاجراء لحماية الرموز داخل التطبيق من الضياع او السرقة وانها تعمل على سلامة التطبيق من القرصنة او التطفل، الى تنفيذ الاجراءات لحماية التطبيقات من الهجوم سواء تطبيقات الويب مثل أي كل المعلومات المتصلة بصورة مباشرة بشبكات الإنترنت، وبالتالي فمن المنطقي أنها تكون مهددة بالهجمات على أمنها السيبراني، وهذا النوع من الأمن السيبراني يهدف للكشف عن البيانات الحساسة التي يجب حمايتها من الهجمات المتوقعة، من خلال برامج مضادات الفيروسات، وجدران الحماية، وعمليات تشفير المعلومات، يكون الاختراق بسبب وجود ثغرات داخل التطبيق او البرنامج التي تستخدم لغزو الخصوصية او سرقة بيانات فردية او لمؤسسة او لدولة(٢٨).

ثالثاً- أمن البنية التحتية: هو حماية الانظمة والاصول المهمة من التهديدات المادية والإلكترونية وأنه إجراء أمني يقوم على أساس حماية البنية التحتية الحيوية للنظام والحد من نقاط الضعف في هذه الأنظمة من فساد وتخريب وإرهاب ويتم وضع خطة طوارئ في حالة استهداف الأنظمة لدى الشركة من قبل مجرمي الإنترنت، وتتراوح التهديدات السيبرانية للبنية التحتية للتكنولوجيا من محاولات التصيد وهجمات البرامج الفدية والى عمليات حجب الخدمة الموزعة(٢٩).

رابعاً- الامن السحابي: وهي الموارد التي توفرها الحوسبة السحابية خدمات لمعالجة المعلومات عبر الانترنيت لتوفير بيئة سحابية امنة، لكون التوجهات الغالبة الآن لمعظم المؤسسات حول العالم هي استخدامها لتكنولوجيا الذكاء الاصطناعي والسحابات التخزينية، وان الحوسبة السحابية تمنح المرونة عند توسيع نطاق عملياتها، ا صبح من اللازم تأمين السحابة الرقمية بسبب احتوائها على كمية بيانات هائلة لهذه المؤسسات(٣٠).

المطلب السادس: الامن السيبراني والتحديات المستقبلية

إذا أردنا ان نتكلم عن التحديات التي تواجه الامن السيبراني المستقبلية فتوجد الكثير من التحديات في ظل التطور السريع في التكنولوجيا، يواجه الامن السيبراني عدة تحديات منها:

اولاً . فيروسات الفدية: هو برنامج خبيث يقيد الوصول إلى نظام الحاسوب الذي يصيبه، ويطالب بدفع فدية لصانع البرنامج من أجل إمكانية الوصول للملفات وهناك انوع منة تقوم بتشفير الملفات على القرص الصلب للنظام وتصيب أجهزة الكمبيوتر وبعدها تمنع المستخدم من الوصول إلى نظام التشغيل أو تشفر جميع البيانات المخزنة على جهاز الكمبيوتر او التصيد الاحتيالي الموجهة، واستغلال الثغرات الامنية من قبل المجرمين، وتعرض رسائل تطلب من المستخدم الدفع باستخدام الابتزاز، ويطلق علية مصطلح برمجة الابتزاز[٣١].

ثانياً . البرمجيات الخبيثة: إنها برامج تم تصميمها للوصول الى اجهزة الكمبيوتر والهواتف من أجل إلحاق الأذى بالمعلومات المخزنة في حواسيب الآخرين من وما يرتبط بها عبر الشبكات، والهدف من هذه البرامج، سرقة المعلومات، الهويات والتجسس ومراقبة والتخريب في المعلومات والبنية الحاسوبية، وهناك أنواع متعددة من البرامج الحاسوبية الخبيثة التي قد تتسلل إلى الحواسيب المختلفة بطرق متعددة، هي متجددة ويبرز الفيروس الحاسوبي Virus Computer كأبرز أنواع هذه البرامج، وإنه برنامج خبيث يستطيع تغيير طريقة عمل الحاسوب مسببا أثرا تخريبيا وعمل هذا الفيروس من خلال إلحاق نفسه مع برامج مشروعة في النظام، و يستطيع الانتقال عبر الشبكات إلى حواسيب أخرى لتوسيع أثر أضراره، ومن البرامج الخبيثة هي الدودة الحاسوبية Computer Warm التي تتميز بأنها تستطيع تنفيذ برنامجها الخبيث دون الحاجة إلى الارتباط ببرامج مشروعة[٣٢].

ثالثاً – هجوم MITM: نوع من البرامج الضارة التي يقوم عن طريقها المهاجم بالتدخل في الاتصال او الرسائل بين الطرفين ليكون الطرف الثالث بيهم دون معرفة الطرفين بذلك، حيث يعتقد المرسل والمستلم انهما يتواصلان مباشرة بسرية تامة دون طرف ثالث يطلع على الرسائل او الاتصال[٣٣].

رابعاً – التهديدات السيبرانية العابرة للحدود: اوضح مدير المرونة الرقمية والامن السيبراني في شركة " PWC" سيمون فيرناشيا، تقرير اوضح فيه ان التوترات الجيوسياسية نتج عنها تهديدات سيبرانية عديدة التي استهدفت البنى التحتية الحساسة، ومن المتوقع ان تكون هناك تهديدات سيبرانية عالمية تهدف الى تخريب الخطوط الامداد الرئيسية مثل الغاز والنفط والبتروكيمياويات وشبكة الكهرباء، ويعرف بهجوم الوسيط.

خامساً – التصيد الاحتيالي: يستهدف التصيد الاحتيالي نقطة الضعف الأساسية في أي نظام أمني وهو العامل البشري يُعتبر من أبرز التحديات التي تواجه الأمن السيبراني ويستخدم أساليب احتيالية لخداع الأفراد أو المؤسسات للحصول على معلومات حساسة، مثل كلمات المرور أو بيانات تسجيل الدخول و يتم ذلك من خلال البريد الإلكتروني المزيف او إنشاء مواقع المزيفة تحاكي المواقع الأصلية لجمع بيانات تسجيل الدخول أو المعلومات الشخصية[٣٤].

المطلب السابع: ابعاد الامن السيبراني

اولاً – الابعاد الاجتماعية: تتجسد الابعاد الاجتماعية للامن السيبراني في تأثير المخاطر الاجتماعية والتهديدات السيبرانية في تشكيل بنية المجتمع حيث ان زيادة الجرائم الإلكترونية تهدد البنية التحتية، وتهدد القيم والاخلاق وهذا يؤدي لازمة ثقة في الاجهزه الامنية والحكومة[٣٥] وكذلك تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بان يعبر عن أفكاره والاطلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن أهمية الأمن السيبراني في حماية وصيانة القيم الجوهرية في المجتمع كالانتماء والعادات والتقاليد، ويهتم البعد الاجتماعي في فهم سلوك المستخدمين والتعامل مع الاثار الاجتماعية للجرائم الإلكترونية وتقديم الدعم الاجتماعي للضحايا وبناء ثقة الافراد بالأمن السيبراني وتحفيز الوعي بالأمن السيبراني وكيفية التعامل مع التكنولوجيا الرقمية[٣٦].

يؤكد البحث ان اهمية البعد الاجتماعي يتجسد في الانعكاس لتأثير الجرائم الإلكترونية والتهديدات الرقمية في نفوس الافراد فلم تعد قضية الامن السيبراني مجرد قضية تقنية او تجارية بل اصبحت اجتماعية ولها اثار واضحية في المجتمعات، حيث يتزايد الشعور بالقلق والتوتر،حول كيفية حماية المعلومات الشخصية من الاستغلال، وهذا الدور يقوم بة الامن السيبراني مما يعزز بناء ثقة بين الافراد وبين المؤسسات الرقمية وكذلك تثقيف الافراد للوعي بمخاطر العالم الالكتروني والتوعية بالتقنيات والتهديدات السيبرانية لمنع وقوع الجرائم الإلكترونية، لتوفير بيئة رقمية امنة، ويجمع البعد الاجتماعي بين القيم الانسانية والجوانب التقنية ودعم التطور التكنولوجي.

ثانياً – الابعاد السياسية: يقوم البعد السياسي للأمن السيبراني على اساس حماية نظام الدولة السياسية وكيانها ومصالحها، وتعني حقها وواجبها في السعي لتحقيق رفاهية شعبيها، وتؤثر التقنيات

في موازين القوى داخل المجتمع ذاته، وانه يمكن استخدام التقنيات في بث البيانات والمعلومات قد يحدث من خلالها زعزعة استقرار امن الدول والحكومات حيث انها يمكن ان تصل بسرعة فائقه الى اكبر عدد من شرائح المجتمع بغض النضر عن صحة هذه البيانات والمعلومات التي تم نشرها، لذلك يجب وضع الادوات والمفاهيم والسياسات الامنية وضمانات الامان والمبادئ التوجيهية لإدارة المخاطر والتدريب والاجراءات والضمان وافضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية والمستخدمين(٣٧).

ثالثاً . الابعاد الاقتصادية: يرتبط الامن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، فهناك تزامن بين الاقتصاد وبين استخدام تقنيات المعلومات، فالترابط المتين بين الاقتصاد والمعرفة ادى الى اعتماد اغلب دول العالم في تعزيز الاقتصاد وازدهاره وتطويره على كافة المستويات وهذا ادى الى ابراز الدور الهام والخطير للأمن السيبراني في حماية الاقتصاد من عمليات القرصنة والسرقة والاحتيال وتقدير تكلفة التهديدات السيبرانية والاضرار المالية المحتملة للهجمات والجرائم الإلكترونية، واستثمار تقنيات الامن السيبراني للحفاظ على المحتويات داخل الالكترونيات(٣٨).

رابعاً- البعد الثقافي: يقوم هذا البعد على حماية الفكر والمعتقدات ويحافظ على العادات والتقاليد والقيم ويعزز ويؤمن انطلاق مصادر القوة الوطنية في كافه الميادين وذلك لمواجهة التهديدات الخارجية والتحديات الداخلية ويوسع قاعده الشعور بالكرامة والحرية والامن والقدرة على تحقيق الرفاهية للمواطنين وتحسين اوضاعهم المالية بصورة مستمرة وان الدور الثقافي هو مهم في تحصين الوطن من الهجمات الثقافية في ظل التطور التكنولوجي وثورة المعلومات وصراع الحضارات ويتضمن البعد الثقافي الفكر والتعليم والاعلام والفنون والادب(٣٩).

خامساً - البعد العسكري: يعمل الامن السيبراني على ربط الوحدات العسكرية بعضها ببعض عبر الفضاء الالكتروني، مما يسهل عملية تبادل المعلومات الذي ينعكس ايجابياً على تحقيق الاهداف العسكرية، اما الاثار السلبية فتتمثل في اختراق النظم العسكرية وسرقة المعلومات الحساسة، وتكمن خطورة هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي الى نشأة الحروب والنزاعات والصراعات المسلحة، وكذلك اختراق المنشأة النووية، وما ينتج عنها من تهديدات لأمن الدول

والحكومات، لذلك ضرورة وجود اطار قانوني في الامن السيبراني من اجل حماية المواقع العسكرية مع ضرورة وجود حماية للاماكن ذات اهمية كبيرة للدولة، ومثال على بعض الاختراقات ما حصل في جورجيا وايران من هجمات سيبرانية واختراقات(٤٠).

سادساً – الابعاد القانونية: يرتبط بالامتثال القانوني المتعلق بالأمن السيبراني وقوانين مكافحة الجرائم الالكتروني وارتباطها بالأنشطة المختلفة التي يقوم بها الافراد والمؤسسات بالقوانين، وعند ظهور المجتمع المعلوماتي ظهرت لدينا قوانين جديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحماية كافة الحقوق فيه بما يتضمن من ابعاد ويقوم الامن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ القوانين والتشريعات(٤١).

المطلب الثامن: الجهود الدولية المبذولة لتعزيز الامن السيبراني

هناك العديد من المؤتمرات الدولية التي ركزت على قضايا الأمن السيبراني وساهمت في تطوير استراتيجيات وحلول للتعامل مع التهديدات السيبرانية المتزايدة. أبرز هذه المؤتمرات:

أولاً– مؤتمر الأمن السيبراني العالمي الخليجي الخامس: يُعقد هذا المؤتمر سنوياً في مدن عالمية مختلفة، ويجمع قادة وخبراء الأمن السيبراني لمناقشة التهديدات الحديثة والتحديات المستقبلية. يركز المؤتمر على تعزيز الأمن الرقمي والتعاون الدولي في التصدي للجرائم السيبرانية.

ثانياً – منتدى الإنترنت العالمي لمكافحة الإرهاب (GIFCT): يركز على التعاون بين الحكومات والمنظمات التقنية الكبرى لمنع انتشار المحتوى الإرهابي على الإنترنت. يهدف المنتدى إلى وضع معايير وتطوير أدوات لرصد المحتوى الضار.

ثالثاً – مؤتمر الاتحاد الدولي للاتصالات حول الأمن السيبراني: ينظمه الاتحاد الدولي للاتصالات التابع للأمم المتحدة، ويهدف إلى تعزيز التعاون الدولي في مجال الأمن السيبراني، خاصة بين الدول النامية والدول المتقدمة.

رابعاً – مؤتمر القمة العالمية لمجتمع المعلومات: تُنظم هذه القمة من قبل الاتحاد الدولي للاتصالات ومنظمات تابعة للأمم المتحدة، وتهدف إلى معالجة قضايا المجتمع المعلوماتي السيبراني لتطوير سياسات واستراتيجيات لحماية المجتمع الرقمي على مستوى العالم(٤٢).

خامساً – مؤتمر الأمن السيبراني لحلف الناتو: ينظمه حلف شمال الأطلسي (الناتو) لبحث سبل تعزيز الأمن السيبراني بين دول الحلف، ويناقش المؤتمر قضايا مثل الحرب السيبرانية، والتجسس الرقمي، وتأمين البنية التحتية الحيوية.

سادساً – مؤتمر الشرق الأوسط للأمن السيبراني: يُعقد سنويًا في منطقة الشرق الأوسط، ويهدف إلى جمع الخبراء وصناع القرار في المنطقة لتبادل المعرفة حول أحدث التهديدات السيبرانية، والتقنيات الدفاعية[٤٣].

المطلب التاسع: نشأة الجريمة الإلكترونية

ان نشأة الجريمة الإلكترونية مرتبطة بتطور تكنولوجيا المعلومات والإنترنت، حيث بدأت في الظهور بشكل ملحوظ مع انتشار استخدام الأجهزة الإلكترونية وان مفهوم الجرائم الإلكترونية مر بتطور تاريخي تبعا لتطورت التقنية واستخداماتها واهميتها، خاصة بعد اعتماد الدول على شبكات الانترنيت والحاسوب بشكل رئيسي وان تلك الجرائم مرت بعده مراحل، والتي يمكن إيجازها على النحو التالي:

المرحلة الاولى السبعينات: تمثلت المرحلة الاولى لأول مره بين الفترة (١٩٧١ -١٩٩٠) حيث ظهرت الجريمة الإلكترونية مع شيوع استخدام الحواسيب في الستينيات والسبعينيات عندما بدأت الحكومات والشركات تعتمد في استخداماتها على الحاسوب وتخزين البيانات المهمة، ومع تزايد استخدام الحواسيب ظهرت هجمات الكترونية بسيطة في محاولة التسلل الى الانظمة بهدف الحصول على المعلومات، في السبعينيات ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر، وظهر عدد قليل من جرائم الحاسوب واشهرها في عام ١٩٨٨ في جامعة "كارنيجي ميلون" ولأول مرة تم انشاء فريق طوارئ للحاسوب الالي حيث تم سرقة ٧٠ مليون دولار من بنك شيكاغو الوطني وعالجت عدداً من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة[٤٤].

المرحلة الثانية التسعينات "ظهور البرامج الضارة والفيروسات":

وفي هذه المرحلة عام ١٩٨٩ م بدأت الجرائم الإلكترونية تتطور وظهرت العديد من الفيروسات والبرامج الضارة التي ساهمت في سرقة المعلومات والبيانات وتعطيل الاجهزة الإلكترونية مثل فيروس "Morris Worm" الذي يعتبر اول فيروس انتشرت في شبكة الانترنيت، وفي هذا الوقت

تبنت اللجنة الوزارية لمجلس اوربا التوصية رقم ٩ (٨٩) الخاص بمواجهة الجرائم الإلكترونية، وبرز مفهوم جديد للجرائم الإلكترونية ارتبط بعمليات اقتحام نظام الكمبيوتر عن بعد، وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات والبرامج(٤٥).

المرحلة الثالثة: وهي مرحلة انتشار الجريمة الإلكترونية وتمثلت في فترة التسعينيات حيث شهدت ارتفاعا هائلا في معدل الجرائم الإلكترونية، وتغييرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعملية دخول الأنظمة واقتحام شبكة المعلومات ووابرز جريمة الكترونية وقعت عام ١٩٩٥م حيث تمكنت عصابة روسيا المحترفة من سرقة عشرة ملايين دولار من مصرف سيتي بنك باستخدام تقنيات الحاسوب الالي وتحويلها الى حسابات في فلندا واسرائيل، وظهرت عمليات الاحتيال عبر الانترنيت، والتجسس السيبراني بين الدول وظهرت الحوسبة السحابية وسرقة الهوية والابتزاز الالكتروني ونشر الافكار العدائية، وفي عام ٢٠١٧ ظهر هجوم الفدية " Wannacry" الذي تسبب بخسائر مادية ضخمة(٤٦).

الاستنتاجات

١. ضرورة حماية المعلومات الشخصية والمالية من السرقة والتسريب، وذلك بسبب وجود عدد كبير من الجيوش الالكترونية التي تحاول ان تخترق المعلومات الشخصية للعديد من الدوائر المهمة والحساسة.
٢. تبين ان هنالك العديد من الجرائم وتشمل البرمجيات الخبيثة، الاحتيالات، والهجمات المنسقة.
٣. هنالك العديد من الدوائر تقوم بعمليات التعليم والتثقيف حول المخاطر وآليات الوقاية من الهجوم المفاجئ وهذا ما يحاول له جاهداً الامن السيبراني ان يتصدى لهُ.
٤. تبي ان هناك العديد من الموظفين يستخدمون أدوات متقدمة مثل جدران الحماية والتشفير لحماية الأنظمة.
٥. هنالك تعاون دولي يحث على تطوير الامن السيبراني لمكافحة الجرائم الإلكترونية تنسيقاً بين الدول لتبادل المعلومات.
٦. تطور أساليب المجرمين واستمرار نقص المحترفين المدربين يشكلان تحديات كبيرة.

الهوامش

(١) جيفري نيونهام، غراهام ايفانس ، قاموس بنغوين للعلاقات الدولية ، دار مركز الخليج للأبحاث ، ٢٠٠٤م، ص٦.

(٢) بول روبنسون، قاموس الامن الدولي ، مركز الامارات للدراسات والبحوث الاستراتيجية ، الطبعة الاولى ، ٢٠٠٩ ، ص٩.

(٣) ابن منظور، لسان العرب، تحقيق عبد الله علي الكبير، القاهرة، دار المعارف، ص١٤٠.

(٤) روحي البعلبكي، المورد، دار العلم للملايين، ط٧، ١٩٩٥، ص٦٣٢.

(٥) يوسف بن ابراهيم السلوم ، معجم المصطلحات العسكرية ، الرياض مكتبة العبيكان، ط١، ٢٠٠٠، ص٤٢٣.

(٦) سراج الدين أحمد امبابي، خالد بن سليمان الغثبر، قاموس مفردات أمن المعلومات ، مركز التميز لأمن المعلوماتي ، متوفر على الموقع https://coeia.ksu.edu.sa/ar/dictionary .

(٧) الاتحاد الدولي للاتصالات: دليل الامن السيبراني للبلدان النامية ، ٢٠٠٧م ، الموجز التنفيدي ، ص٤٤ .

(٨) ابن منظور، لسان العرب، مصدر سابق، ج١٢، ص ٩٢.

(٩) ابن عطا الله الاسكندري، تاج العروس، مكتبة الروضة الشريفة للبحث العلمي ،٢٠٠٦م ، ج٨، ص ٢٢٤

(١٠) محمد عبدالله الوريكات، مبادئ علم الاجرام ، كليه الحقوق . جامعه عمان الاهلية ، ط١، ٢٠٠٨ ، ص٦٣.

(١١) د. رميس بهنام ، علم الاجرام ، دار المعارف الاسكندرية للنشر، ص٣٠.

(١٢) غنام محمد غنام ، علم الاجرام والعقاب ، دار الفكر والقانون ، ط١، ٢٠١٥ ، ص١٠.

(١٣) محمد ابراهيم الدسوقي، مبادئ علم الاجرام والعقاب، مكتبة الرشد، ٢٠١٦، ص١٠-١٩.

(١٤) معجم المعاني الجامع – معجم الكتروني، متوفر على الموقع التالي https://www.almaany.com. تمت زيارة الموقع في ٢٠٢٤ /١٠/ ٢٣

(١٥) محمود احمد القرعان ، الجريمة الالكترونية ، عمان ، دار وائل للنشر والتوزيع ، ٢٠١٦م ، ص٢٥.

(١٦) سيد علي السيد محمد ، الجرائم الالكترونية، كلية الآداب جامعة المينا ،الاسكندرية ، ٢٠٢٠م ، ص١٩.

(١٧) بول روبنسون ، قاموس الامن الدولي ، مركز الامارات للبحوث والدراسات الاستراتيجية ، ط١، ٢٠٠٩ ، ص٨٥.

(١٨) ابن منظور، لسان العرب، بيروت للطباعة والنشر ، ١٩٩٥ ، ص١٣٧٤.

(١٩) حيدر فالح سليمان، مقدمه في الامن السيبراني ، دار الكتب والوثائق، بغداد ، ٢٠٢٤ ، ص٧٠.

(٢٠) أحمد مختار عمر ، معجم اللغة العربية المعاصرة ، دار النهضة، ط١، ٢٠٠٨، مصر، ص٢٣٢٩.

(٢١) د. شيماء تركان صالح ، الامن السيبراني العراقي والتهديدات السيبرانية ... الارهاب السيبراني انموذجاً ، جامعة النهرين / كلية العلوم السياسية ، بحث منشور ، مجلة الاكاديمية العالمية، ٢٠٢٣.

(٢٢) ايمن محمد فارس الدنف ، واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها ، بحث منشور ، مؤسسة انجازات ، الجامعة الاسلامية غزة ،كلية التجارة ، ٢٠١٣م.

(٢٣) Ali Fauz ، Information Securety Threats Against Mobaile Phone Services ، Lolita University of Technology، Iraqi Academic Journal, 2009.

(٢٤) حيدر فالح سلمان ، مقدمه في الامن السيبراني، دار الكتب والوثائق بغداد ، ٢٠٢٣، ص٢٣.

(٢٥) المصدر نفسه، ص١٦.

(٢٦) المصدر نفسه، ص١٦.

(٢٧) محمد عبدالله شاهين محمد ، الامن السيبراني ونظم حماية المعلومات ، المركز الاكاديمي للنشر ومكتبة الدراسات العربية للنشر والتوزيع ، ٢٠٢٥ ، ، ص٢١.

* الدخول غير المصرح به هو الوصول إلى الأنظمة أو البيانات أو الموارد الرقمية دون إذن رسمي. وهو فعل غير قانوني ويشكل تهديدًا للأمن السيبراني، و يؤدي إلى سرقة المعلومات، أو التخريب المتعمد للبنية التحتية الرقمية أو التلاعب بالبيانات.

(٢٨) الدكتور همايون باخت، الامن السيبراني، ٢٠٢٠ ، كتاب الكتروني متوفر على الموقع التالي https://www.google.iq/books/edition تمت زيارة الموقع في ١/١١/٢٠٢٤ ص ٨ .

(٢٩) والفرص رعد خضير صليبي، تعزيز الامن السيبراني في العراق: التحديات، جامعة بغداد ، مركز الدراسات الاستراتيجية والدولية ، مجلة الدراسات الدولية ، ٢٠٢٤، ص٥١٦.

(٣٠) حيدر فالح سليمان، مصدر سابق، ص٧٥.

(٣١) بدر عدنان احمد الخبيزي ، تحديات وتهديدات الامن السيبراني وكيفية التغلب عليها ، جامعة عين الشمس/كلية الآداب، حث منشور، المجلد٥١، ٢٠٢٣، ص٢٤٢.

(٣٢) المصدر نفسه ، ص٢٤٣.

(٣٣) هيئة الاعلام / قسم الدراسات والاتصال والعلاقات العامة، الامن السيبراني، مجلة هيئة الاعلام ، ٢٠٢١، ص١١.

(٣٤) صفاء عبدالخالق زمان ، امنه عبدالله عيادة ، تحديات الامن السيبراني وتأثيراته على هيئات ومؤسسات دول مجلس التعاون لدول الخليج العربي ، التقرير الاستراتيجي / العدد٢٦، مركز الدراسات الخليج والجزيرة العربية ، جامعة الكويت ، ٢٠٢٤، ص٢٧.

(٣٥) اسلام فوزي، الامن السيبراني: الابعاد الاجتماعية والقانونية تحليل سوسيولوجي ، بحث منشور ، المجلة الاجتماعية القومية، المجلد السادس، العدد٢، ص١٠٤ .

(٣٦) عاطف حسن، الأمن السيبراني حتمية فرضها التطور، مجلة البنك المركزي المصري، مقال منشور في مجلة الكترونية ، ٢٠٢٤ ، ص٣.

(٣٧) ناظم حسن رشيد ، الامن السيبراني منظور التدقيق الداخلية ، جامعة الحمدانية كلية الإدارة والاقتصاد،، دار ابن الاثير للطباعة والنشر ،٢٠٢٢، ص٣٨.

(٣٨) ايات فاخر محمد العلوي ، الامن السيبراني العراقي : الواقع وافاق المستقبل ،بحث منشور، المجلة السياسية الدولية ، الجامعة المستنصرية / كلية العلوم السياسية ،بغداد ، العدد٥٨، ص٢٩٢، ٢٩٣.

(٣٩) عاصي حسين حمود، سهاد عادل احمد، اثر الثقافة الموجهة على امن وهوية المجتمع العراقي، مجلة الفراهيدي ، العدد ٢٣ ، بغداد /٢٠١٥ ، ص ٣٧٢.

(٤٠) فارس محمد العمارات، الامن السيبراني، المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، ٢٠٢٢، ص٣٠.

(٤١) محمد عبدالله شاهين، الامن السيبراني ونظم حماية المعلومات، مصدر سابق، ص٦٢.

(٤٢) جاسم محمد عز الدين / حازم حمد موسى، الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي، كلية القانون والعلاقات الدولية / كلية العلوم السياسية، جامعه الموصل ،٢٠٢٤، ص٦.

(٤٣) المصدر نفسه، ص٧.

(٤٤) غادة العربي نصار: الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة ٢٠١٧، ص ٩.

(٤٥) اسراء جبريل مراعي، الجرائم الالكتروني، مجلة الدراسات الاعلامية، ٢٠١٨، ص١٠.

(٤٦) هشام بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والاستراتيجية، ٢٠١٢، ص: ٦، ٧.

المصادر باللغة العربية

١. ابن عطا الله الاسكندري، تاج العروس، مكتبة الروضة الشريفة للبحث العلمي،٢٠٠٦م، ج٨.
٢. ابن منظور، لسان العرب، بيروت للطباعة والنشر، ١٩٩٥.
٣. ابن منظور، لسان العرب، تحقيق عبد الله علي الكبير، القاهرة، دار المعارف.
٤. الاتحاد الدولي للاتصالات: دليل الامن السيبراني للبلدان النامية، ٢٠٠٧م، الموجز التنفيذي.
٥. أحمد مختار عمر، معجم اللغة العربية المعاصرة، دار النهضة، ط١، ٢٠٠٨، مصر.
٦. اسراء جبريل مراعي، الجرائم الالكتروني، مجلة الدراسات الاعلامية، ٢٠١٨.

٧. اسلام فوزي، الامن السيبراني: الابعاد الاجتماعية والقانونية تحليل سوسيولوجي، بحث منشور، المجلة الاجتماعية القومية، المجلد السادس، العدد٢.

٨. ايات فاخر محمد العلوي، الامن السيبراني العراقي: الواقع وافاق المستقبل، بحث منشور، المجلة السياسية الدولية، الجامعة المستنصرية / كلية العلوم السياسية، بغداد، العدد٥٨.

٩. ايمن محمد فارس الدنف، واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، بحث منشور، مؤسسة انجازات، الجامعة الاسلامية غزة، كلية التجارة، ٢٠١٣م.

١٠. بدر عدنان احمد الخبيزي، تحديات وتهديدات الامن السيبراني وكيفية التغلب عليها، جامعة عين الشمس/كلية الآداب، حث منشور، المجلد٥١، ٢٠٢٣.

١١. بول روبنسون، قاموس الامن الدولي، مركز الامارات للبحوث والدراسات الاستراتيجية، ط١، ٢٠٠٩.

١٢. بول روبنسون، قاموس الامن الدولي، مركز الامارات للدراسات والبحوث الاستراتيجية، الطبعة الاولى، ٢٠٠٩.

١٣. جاسم محمد عز الدين / حازم حمد موسى، الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي، كلية القانون والعلاقات الدولية / كلية العلوم السياسية، جامعه الموصل،٢٠٢٤.

١٤. جيفري نيونهام، غراهام ايفانس، قاموس بنغوين للعلاقات الدولية، دار مركز الخليج للأبحاث، ٢٠٠٤م.

١٥. حيدر فالح سلمان، مقدمه في الامن السيبراني، دار الكتب والوثائق بغداد، ٢٠٢٣م.

١٦. حيدر فالح سليمان، مقدمه في الامن السيبراني، دار الكتب والوثائق، بغداد، ٢٠٢٤.

١٧. الدكتور همايون باخت، الامن السيبراني، ٢٠٢٠، كتاب الكتروني متوفر على الموقع التالي .https://www.google.iq/books/edition

١٨. رميس بهنام، علم الاجرام، دار المعارف الاسكندرية للنشر.

١٩. روحي البعلبكي، المورد، دار العلم للملايين، ط٧، ١٩٩٥م.

٢٠.سراج الدين أحمد امبابي، خالد بن سليمان الغثبر، قاموس مفردات أمن المعلومات، مركز التميز لأمن المعلوماتي، متوفر على الموقع https://coeia.ksu.edu.sa/ar/dictionary .

٢١.سيد علي السيد محمد، الجرائم الالكترونية، كلية الآداب جامعة المينا، الاسكندرية، ٢٠٢٠م.

٢٢.شيماء تركان صالح، الامن السيبراني العراقي والتهديدات السيبرانية ... الارهاب السيبراني انموذجاً، جامعة النهرين / كلية العلوم السياسية، بحث منشور، مجلة الاكاديمية العالمية، ٢٠٢٣.

٢٣.صفاء عبدالخالق زمان، امنه عبدالله عيادة، تحديات الامن السيبراني وتأثيراته على هيئات ومؤسسات دول مجلس التعاون لدول الخليج العربي، التقرير الاستراتيجي / العدد٢٦، مركز الدراسات الخليج والجزيرة العربية، جامعة الكويت، ٢٠٢٤.

٢٤.عاصي حسين حمود، سهاد عادل احمد، اثر الثقافة الموجهة على امن وهوية المجتمع العراقي، مجلة الفراهيدي، العدد ٢٣، بغداد /٢٠١٥.

٢٥.عاطف حسن، الأمن السيبراني حتمية فرضها التطور، مجلة البنك المركزي المصري، مقال منشور في مجلة الكترونية، ٢٠٢٤.

٢٦.غادة العربي نصار: الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة ٢٠١٧.

٢٧.غنام محمد غنام، علم الاجرام والعقاب، دار الفكر والقانون، ط١، ٢٠١٥.

٢٨.فارس محمد العمارات، الامن السيبراني، المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، ٢٠٢٢.

٢٩.محمد ابراهيم الدسوقي، مبادئ علم الاجرام والعقاب، مكتبة الرشد، ٢٠١٦.

٣٠.محمد عبدالله الوريكات، مبادئ علم الاجرام، كليه الحقوق . جامعه عمان الاهلية، ط١، ٢٠٠٨.

٣١.محمد عبدالله شاهين محمد، الامن السيبراني ونظم حماية المعلومات، المركز الاكاديمي للنشر ومكتبة الدراسات العربية للنشر والتوزيع، ٢٠٢٥.

٣٢.محمود احمد القرعان، الجريمة الالكترونية، عمان، دار وائل للنشر والتوزيع، ٢٠١٦م.

٣٣.معجم المعاني الجامع – معجم الكتروني، متوفر على الموقع التالي https://www.almaany.com.

٣٤.ناظم حسن رشيد، الامن السيبراني منظور التدقيق الداخلية، جامعة الحمدانية كلية الإدارة والاقتصاد، دار ابن الاثير للطباعة والنشر،٢٠٢٢

٣٥.هشام بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والاستراتيجية، ٢٠١٢.

٣٦.هيئة الاعلام / قسم الدراسات والاتصال والعلاقات العامة، الامن السيبراني، مجلة هيئة الاعلام، ٢٠٢١.

٣٧.والفرص رعد خضير صليبي، تعزيز الامن السيبراني في العراق: التحديات، جامعة بغداد، مركز الدراسات الاستراتيجية والدولية، مجلة الدراسات الدولية، ٢٠٢٤.

٣٨.يوسف بن ابراهيم السلوم، معجم المصطلحات العسكرية، الرياض مكتبة العبيكان، ط١، ٢٠٠٠.

المصادر باللغة الانجليزية

1. Ahmed Mokhtar Omar, Dictionary of Contemporary Arabic Language, Dar Al-Nahda, 1st Edition, 2008, Egypt.
2. Ali Fauz, Information Securety Threats Against Mobaile Phone Services, Lolita University of Technology, Iraqi Academic Journal, 2009.
3. and Opportunities Raad Khudair Salibi, Enhancing Cybersecurity in Iraq: Challenges, University of Baghdad, Center for Strategic and International Studies, Journal of International Studies, 2024.
4. Assi Hussein Hammoud, Suhad Adel Ahmed, The Impact of Directed Culture on the Security and Identity of Iraqi Society, Al-Farahidi Magazine, Issue 23, Baghdad / 2015.
5. Atef Hassan, Cybersecurity is an Imperative Imposed by Evolution, Central Bank of Egypt Magazine , article published in an electronic magazine, 2024.
6. Ayat Fakher Muhammad Al-Alawi, Iraqi Cybersecurity: Reality and Future Prospects, published research, International Political Journal, Al-Mustansiriya University / College of Political Science, Baghdad, No. 58.
7. Ayman Muhammad Fares Al-Danaf, The Reality of Information Systems Security Management in the Technical Colleges in the Gaza Strip and Ways to Develop Them, Published Research, Injazat Foundation, Islamic University of Gaza, Faculty of Commerce, 2013.

8. Badr Adnan Ahmed Al-Khubaizi, Cybersecurity Challenges and Threats and How to Overcome Them, Ain Shams University / Faculty of Arts, Publication Urge, Volume 51, 2023.
9. Comprehensive Dictionary of Meanings – an electronic dictionary, available on the following website https://www.almaany.com.
10. Dr. Humayun Bakht, Cybersecurity, 2020, e-book available at the following website https://www.google.iq/books/edition.
11. Esraa Jibril Marai, Cybercrime, Journal of Media Studies, 2018.
12. Faris Mohammed Al-Amarat , Cyber Security, Concept and Challenges of the Age, Dar Al-Khaleej for Publishing and Distribution, 2022.
13. Ghada Elaraby Nassar: Terrorism and Cybercrime, Elaraby for Publishing and Distribution, Cairo 2017.
14. Ghannam Muhammad Ghannam, Criminology and Punishment, Dar Al-Fikr wal-Qanoon, 1st Edition, 2015.
15. Haider Faleh Salman, Introduction to Cybersecurity, House of Books and Archives, Baghdad, 2023.
16. Haider Faleh Suleiman, Introduction to Cybersecurity, Dar Al-Kutub and Documents, Baghdad, 2024.
17. Hisham Bashir, International Mechanisms to Combat Cybercrime, International Center for Future and Strategic Studies, 2012.
18. Ibn Atallah Al-Iskandari, Taj Al-Arous, Al-Rawdah Al-Sharifa Library for Scientific Research, 2006, vol. 8.
19. Ibn Manzur, Lisan Al Arab, Beirut Printing and Publishing, 1995.
20. Ibn Manzur, Lisan al-Arab, edited by Abdullah Ali al-Kabir, Cairo, Dar al-Maaref.
21. International Telecommunication Union : Cybersecurity Guide for Developing Countries , 2007, Executive Brief.
22. Islam Fawzy, Cybersecurity: Social and Legal Dimensions: A Sociological Analysis, Published Research, National Social Journal, Volume VI, Issue 2.
23. Jassim Mohammed Ezz El-Din / Hazem Hamad Musa, The Legal Nature of Cyber Wars and Conflicts from the Perspective of International Law, College of Law and International Relations / College of Political Science, University of Mosul, 2024.
24. Jeffrey Newham, Graham Evans, Penguin Dictionary of International Relations, Gulf Research Center, 2004.
25. Mahmoud Ahmed Al-Quran, Cybercrime, Amman, Dar Wael for Publishing and Distribution, 2016.
26. Media Commission / Department of Studies, Communication and Public Relations , Cybersecurity, Media Commission Magazine, 2021.

27. Mohamed Ibrahim El-Desouky, Principles of Criminology and Punishment, Al-Rushd Library, 2016.
28. Mohammed Abdullah Al-Wreikat, Principles of Criminology, Faculty of Law, Al-Ahliyya Amman University, 1st Edition, 2008.
29. Mohammed Abdullah Shaheen Mohamed, Cybersecurity and Information Protection Systems, Academic Center for Publishing and Arab Studies Library for Publishing and Distribution, 2025.
30. Nazem Hassan Rashid, Cybersecurity: Internal Audit Perspective, Al-Hamdaniya University, College of Administration and Economics, Dar Ibn Al-Atheer for Printing and Publishing, 2022
31. Paul Robinson, International Security Dictionary, Emirates Center for Research and Strategic Studies, 1st Edition, 2009.
32. Paul Robinson, International Security Dictionary, Emirates Center for Strategic Studies and Research, First Edition, 2009.
33. Ramis Behnam, Criminology, Dar Al-Maaref Alexandria Publishing.
34. Ruhi Al-Baalbaki, Al-Mawrid, Dar Al-Ilm Li Malayin, 7th Edition, 1995 AD.
35. Safaa Abdulkhaleq Zaman, Amna Abdullah Iyada, Cybersecurity Challenges and its Effects on the Bodies and Institutions of the Cooperation Council for the Arab States of the Gulf, Strategic Report / Issue 26, Center for Gulf and Arabian Peninsula Studies, Kuwait University, 2024.
36. Sayed Ali El-Sayed Mohamed, Cybercrime, Faculty of Arts , El-Mina University, Alexandria, 2020.
37. Shaima Turkan Saleh, Iraqi Cybersecurity and Cyber Threats ... Cyber terrorism as a model, Al-Nahrain University / College of Political Science, published research, Journal of the International Academy, 2023.
38. Sirajuddin Ahmed Imbabi, Khalid bin Suleiman Al-Ghathbar, Dictionary of Information Security Vocabulary, Center of Excellence for Information Security, available on the https://coeia.ksu.edu.sa/ar/dictionary website .
39. Yusuf bin Ibrahim Al-Salloum, Dictionary of Military Terms, Riyadh Obeikan Library, 1st Edition, 2000.