Researcher Journal for Legal Sciences, ISSN: 5960-2706, Vol. 6, No. 1, June, 2025, Pages 53-62
DOI: https:// doi.org/10.37940/JRLS.2025.6.1.3

Mechanisms of the United Nations for Achieving Cybersecurity and Their Impact on Iraqi Legislation

Assist. Prof. Dr. Hameedah Ali Jaber
University of Baghdad / College of Political Science
hameedah.a@copolicy.uobaghdad.edu.iq

Article Info.

Article Progress:

Received
28/1/2025

Accepted
25/2/2025

Publishing
25/6/2025

First Author
https://orcid.org/0009-0003-7818-4495

Abstract

In a constantly changing world, the only constant is change. With the emergence of various forms and types of cyber threats targeting devices and networks, cybersecurity risks have become multifaceted. These risks do not only affect individuals and organizations but also extend to jeopardizing the interests of nations and governments, exposing them to breaches, violations, and dangers. Hence, the need to protect cybersecurity has become urgent to maintain the confidentiality of information across its various types and domains. This requires adopting all necessary measures and actions to deter malicious actors. From this perspective, the importance of researching the mechanisms and strategies adopted by the United Nations to maintain cybersecurity comes to light. The research aims to highlight the most significant decisions and recommendations related to this issue, in addition to examining the regional role in this domain, including the resolutions and measures taken to protect cybersecurity. The study also seeks to analyze the impact of the international and regional roles in achieving cybersecurity through the measures and strategies adopted by the General Assembly and the Security Council. Additionally, the research will shed light on Iraqi legislation, clarifying the key measures and strategies implemented to ensure cybersecurity in Iraq.

Citation: Hameedah Ali Jaber, Mechanisms of the United Nations for Achieving Cybersecurity and Their Impact on Iraqi Legislation, Researcher Journal for Legal Sciences, ISSN: 5960-2706, Vol. 6, No. 1, June, 2025, Pages 53-62
DOI: https:// doi.org/10.37940/JRLS.2025.6.1.3

Publisher: **Publisher: College of Law, University of Fallujah**

Keywords: Cybersecurity, United Nations, Security Council, Iraqi Legislation، strategies".

اليات الأمم المتحدة لتحقيق الامن السيبراني وأثرها على التشريعات العراقية

أ.م.د. حميدة علي جابر
جامعة بغداد/ كلية العلوم السياسية- بغداد- العراق
hameedah.a@copolicy.uobaghdad.edu.iq

معلومات المقالة

تاريخ الاستلام
٢٠٢٥/١/٢٨

تاريخ القبول
٢٠٢٥/٢/٢٥

تاريخ النشر
٢٠٢٥/٦/٢٥

الخلاصة

في ظل عالم متغير، يُعدّ الثبات الوحيد هو التغيير. ومع ظهور أنواع وأشكال مختلفة من التهديدات السيبرانية التي تستهدف الأجهزة والشبكات، أصبحت مخاطر الأمن السيبراني متعددة الأوجه. لا تقتصر هذه المخاطر على الأفراد والمؤسسات فحسب، بل تتعداها إلى تعريض مصالح الدول، والحكومات للاختراق، والانتهاك، والخطر. لذلك، باتت الحاجة مُلحّة إلى حماية الأمن السيبراني للحفاظ على سرية المعلومات بمختلف أنواعها ومجالاتها. يتطلب ذلك اتخاذ جميع التدابير والإجراءات اللازمة لكف أيدي العابثين. من هذا المنطلق، تبرز أهمية البحث في آليات واستراتيجيات الأمم المتحدة التي تم تبنيها للحفاظ على الأمن السيبراني. يهدف البحث إلى بيان أهم القرارات والتوصيات ذات الصلة، بالإضافة إلى استعراض الدور الإقليمي في هذا الجانب، بما يشمل القرارات والإجراءات المتخذة لحماية الأمن السيبراني. كما يسعى البحث إلى تحليل انعكاس الدور الأممي والإقليمي في تحقيق الأمن السيبراني، عبر التدابير والاستراتيجيات التي تبنتها الجمعية العامة ومجلس الأمن. وسيتم أيضًا تسليط الضوء على التشريعات العراقية، مع توضيح أبرز الإجراءات والاستراتيجيات المتخذة لضمان الأمن السيبراني في العراق.

الكلمات المفتاحية: الأمن السيبراني، الأمم المتحدة، مجلس الأمن، التشريعات العراقية، الاستراتيجيات.

١. المقدمة

أصبح نجاح أي هيئة أو مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات. ومع ذلك، فإن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات تواجه مخاطر متعددة بين الحين والآخر. تتعرض هذه الأنظمة لأنواع مختلفة من خروقات المعلومات، كما تقع ضحية لأنشطة إجرامية، مثل هجمات الهاكرز التي تعطل خدماتها وتدمر ممتلكاتها.لذلك، أصبحت قضية أمن وحماية المعلومات واحدة من أهم القضايا في عصرنا الحالي، وهو "عصر الثورة الصناعية الرابعة."

١-١- اهمية البحث:

في سياق الحوسبة، يشهد الأمن السيبراني تحولات هائلة على مستوى التكنولوجيا وعملياتها في العصر الحالي، حيث يلعب علم البيانات دورًا رياديًا في قيادة هذا التغيير. ومع الانتشار الواسع للإنترنت، أصبح الأمن السيبراني واحدًا من أكبر احتياجات العالم، نظرًا لما تشكله تهديداته من خطورة كبيرة على أمن الدول. ولا يقتصر هذا التحدي على الحكومات فقط، بل يتطلب أيضًا نشر الوعي بين الأفراد حول أهمية تحديث إعدادات أمان الأنظمة والشبكات بشكل دوري، بالإضافة إلى استخدام برامج مكافحة الفيروسات المناسبة لضمان حمايتها من الفيروسات والبرمجيات الضارة. بناءً على ذلك، تتزايد الحاجة إلى البحث في الدور الأممي والإقليمي والإجراءات التي اتُّخذت لحماية الأمن السيبراني وتعزيزه، وكذلك دراسة مدى تأثير هذه الآليات والاستراتيجيات على الواقع العراقي.

١-٢- هدف البحث:

يهدف هذا البحث إلى فهم كيف تسهم آليات الأمم المتحدة في تعزيز الأمن السيبراني عالميًا، وما مدى تأثيرها على القوانين العراقية. كما يسعى إلى معرفة إن كانت التشريعات العراقية تواكب المعايير الدولية، وما التحديات التي تواجهها في هذا المجال، مع اقتراح حلول لتطويرها وحماية الفضاء الرقمي في العراق بشكل أفضل.

١-٣- اشكالية البحث: فتتلخص بعدة تساؤلات:

- ما ذا يعني الأمن السيراني وماهي ماهيته؟
- ما مدى فعالية الاليات والاستراتيجيات والجهود الدولية والوطنية لحماية الامن السيبراني وتحقيقه؟
- هل نجعت الاليات والاستراتيجيات العراقية في حماية الامن السيبراني وما مدى موائمتها للجهود الدولية العالمية والاقليمية المتخذة بهذا المضمار؟

١-٤- منهجية البحث:

فقد اعتمد الباحث على المنهج الاستقرائي عبر قراءة نصوص الاتفاقيات والتدبر في الاستراتيجيات والقرارات والتوصيات المتخذة من قبل اجهزة الامم المتحدة لحماية الامن السيراني، وكذلك قراءة مواد القوانين والقرارات العراقية الهادفة لحماية الامن السيبراني, كما اعتمد الباحث المنهج التحليلي من خلال تحليل النصوص القانونية والاطار العملي للأليات والاستراتيجيات الدولية والوطنية الرامية لتحقيق الامن السيبراني, وذلك لإظهار وتوضيح النقص والفراغ الذي يعتري هذه الاليات والاستراتيجيات.

١-٥- هيكلية البحث:

قسمت الدراسة الى مبحثين في المبحث الاول نتناول فيه مفهوم الامن السيبراني وتمييزه عما يشتبه به وقسم هذا المبحث الى مطلبين في المطلب الاول سنتناول تعريف الامن السيبراني وفي المطلب الثاني سوف نتناول تمييز الأمن السيبراني عما يشتبه به، اما المبحث الثاني سنتناول الاليات الدولية والوطنية في تحقيق الامن السيراني ويقسم الى مطلبين في المطلب الاول سنتناول الاليات الدولية لتحقيق الامن السيبراني وفي المطلب الثاني سنتناول الاليات الوطنية لتحقيق الامن السيبراني.

٢- مفهوم الامن السيبراني وتمييزه عما يشتبه به

لغرض الوقوف على ما يتضمنه مفهوم الامن السيبراني من معاني ومحددات وابعاد لابد من تعريفه وهذا ما سنتناوله في الفرع الاول، وكذلك لابد من تمييزه وتميزه عما يشتبه به وهذا ما سنتناوله في الفرع الثاني.

٢-١- تعريف الامن السيبراني

أن ظهور الجرائم السيبرانية يوجب على الدول بذل الجهود الكبيرة لتحقيق الأمن السيبراني وقبل تعريف الامن السيبراني لابد من التطرق إلى تعريف كلمة الأمن أولا ومن ثم تعريف الامن السيبراني ثانيا.

٢-١-١- تعريف الامن

الامن لغة: كما جاء في معجم المعاني الجامع انه من الفعل أمن: أي اطمأن ولم يخف وهو الطمأنينة وعدم الخوف والثقة وعدم الخيانة.

اما تعريف الامن اصطلاحا: فقد عرفه البعض: بانه "القدرة التي تتمكن بها الدولة من إطلاق مصادر قوتها الاقتصادية والعسكرية في شتى المناحي لمواجهة مصادر الخطر في الداخل والخارج في حالتي السلم والحرب، مع استمرار الانطلاق المؤمن لتلك القوى الحاضر والمستقبل" (١).

وبالنسبة للتعريف الاجرائي للأمن: فيعرفه البعض بأنه: "شعور الإنسان بالطمأنينة على نفسه وما يتصل به من عرض ومال ومسكن وملبس وطعام، وإذا ما تم إضافة لفظ الأمن إلى أي مجال من المجالات انحصر معنى الأمن فيما أضيف إليه"(٢).

٢-١-٢- تعريف الامن السيبراني(٣).

عرف جانب من الفقه الامن السيبراني بانه: "التقنيات والإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبيانات من الدخول غير القانوني ونقاط الضعف والهجمات المنقولة عبر الإنترنت من قبل الجانحين السيبرانيين"(٤). وعرفه جانب اخر بانه:" وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة". وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الأمن السيبراني لعام ٢٠١٠- ٢٠١١ بأنه": مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة ا لمخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"(٥).

وعرفه اخرون على انه: "جميع العمليات التي تستهدف حماية اصول تكنلوجيا المعلومات المكونة للفضاء السيبراني"(٦). وقدمت وزارة الدفاع الأمريكية "البنتاغون تعريفا دقيقا لمصطلح الأمن السيبراني، فاعتبرته:" جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف انواع الجرائم: الهجمات، التخريب، التجسس والحوادث"(٧). اما الهيئة الوطنية للأمن السيبراني فقد عرفته بانه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من عتاد وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع"(٨).

تأسيسا على ذلك يعرف الامن السيبراني، انطلاقا من اهدافه بأنه: النشاط الذي يضمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويؤمن الحد من الخسائر والاضرار الناتجة عن تحقيق المخاطر والتهديدات، كما يوفر إمكانية اعادة الوضع الى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، ولا تتحول الأضرار الى خسائر دائمة"(٩).

---

(١) خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي، بحث منشور في مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون, يوليو ٢٠٢٢,ص٩٩٣.

(٢) المصدر نفسه ، ص٩٩٥.

(٣)الأمن السيبراني هو مصطلح مستمد من كلمتي **(Cyber Security)**، حيث تُعَدُّ كلمة "سيبر" ذات أصل لاتيني وتعني الأمن المعلوماتي. وعليه، يشير الأمن السيبراني إلى مفهوم أشمل وأوسع من أمن المعلومات. يمكن تعريف الأمن السيبراني بأنه مجموعة الوسائل التقنية والإدارية التي تُستخدم لمنع الاستخدام غير المصرح به، والحد من سوء استغلال نظم الاتصالات والمعلومات الإلكترونية، بالإضافة إلى استعادتها عند الحاجة. يهدف الأمن السيبراني إلى ضمان توافر واستمرارية عمل نظم المعلومات، وحماية سرية وخصوصية البيانات الشخصية، وتأمين الأفراد من المخاطر السيبرانية. ينظر: نوري حمد خاطر، حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، بحث منشور في مجلة المنارة، العدد (٢)، كانون الثاني لعام ٢٠١٢, ص٣٥.

)4 (K. K. Panigrahi , Information Security and Cyber Law , published by tutorials point ,2015, p.1.

(٥) دليل الامن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام ٢٠١٠,ص٤٢١.

(٦) خالد الشايع، الامن السيبراني مفهومه وخصائصه وسياساته، دار العالمية، الطبعة الاولى, ٢٠١٨,ص٢٥.

(٧) خالد ظاهر عبد الله جابر السهيل المطيري، المصدر السابق، ص٩٩٦.

(٨) الأمن السيبراني، مقال منشور على الموقع الإلكتروني https://political-encyclopedia.org/dictionary تاريخ الزيارة ٢٠٢٤/١١/١٨.

(٩) سعيد عبد اللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنيت، دار النهضة العربية، القاهرة،ط٤, ص٢١٤.

يلاحظ مما سبق أنه على الرغم من عدم وجود تعريف موحد للأمن السيبراني، إلا أنه تم الاتفاق على الأهمية القصوى التي يلعبها في توفير الحماية للبيانات والمعلومات الاستراتيجية لمؤسسات الدولة والشركات، والتقليل من الجرائم الإلكترونية. كما يُعنى بحماية خصوصية الأفراد، حيث يؤدي اختراقها إلى تهديد أمن المؤسسات والأفراد، مما يسبب خسائر وأضراراً قد تهدد الأمن القومي للدول.

٢-٢- تمييز الامن السيبراني عما يشتبه به

حتى لا يختلط مفهوم الامن السيبراني بغيره من المفاهيم المتداخلة معه فلابد من تميزه عن مفهوم امن المعلومات

اولا ومن ثم تميزه عن عدة مفاهيم ترتبط معه ثانيا.

٢-٢-١- تمييز الامن السيبراني عن امن المعلومات

يقصد بأمن المعلومات بانه: العلم الذي يهتم بدراسة وسائل حماية البيانات المخزنة في الحاسوب وأنظمة الاتصالات ويبحث في طرق التصدي للمحاولات غير المشروعة للوصول إلى البيانات، أو نقلها أو تعديلها أو إلحاق الضرر ببرمجيات حماية البيانات (١٠).

كما يعرف امن المعلومات بانه:" حماية بيانات المؤسسة ويعتمد على ثلاث محاور رئيسية يرمز لها (CIA)(١١) .وهي السرية، سلامة المعلومة واتاحة المعلومة في أي وقت"(١٢). وهو يحمي سلامة وخصوصية البيانات سواء في مرحلة التخزين او التناقل.

ومن خلال التعريفات السابقة للآمن السيبراني فأنه يشمل الأمن الإلكتروني والأمن الرقمي، ويمكن تعريف الأمن السيبراني بأنه: مجموعة من التدابير التي تُتخذ لحماية شبكات الاتصالات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، بما يشمل مكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، بالإضافة إلى البيانات التي تحتويها. يهدف الأمن السيبراني إلى الحماية من المخاطر المحتملة عبر إجراءات وقائية مسبقة، أو التصدي لأي اختراق، أو هجوم سيبراني، أو تعطيل، تعديل، دخول، استخدام، أو استغلال غير قانوني. كما يُعنى بحماية البنى التحتية الحساسة للدولة من التهديدات السيبرانية، مثل هجمات الروبوتات. وتشمل هذه الجهود كل الجرائم السيبرانية، سواء كانت صادرة عن جهات حكومية أو غير حكومية، وتُنظم وفقاً للقوانين واللوائح الوطنية المعتمدة في الدولة. وينظم الإجراءات الخاصة بالأمن السيبراني وفقا للقوانين واللوائح الوطنية للدولة (١٣).

الأمن السيبراني وأمن البيانات ليسا مصطلحين مترادفين بسبب اختلاف مجالات اهتمام كل منهما. أمن المعلومات يركز على حماية البيانات التي تكون مرفقة بالفعل على المنصات الإلكترونية، بينما يهتم الأمن السيبراني بمنع اختراق هذه البيانات واستخدامها بشكل غير مصرح به. يُطبق الأمن السيبراني شروط الخصوصية التي تحددها الجهة المالكة للتطبيق، مما يسمح لأنظمتها بالوصول إلى المعلومات المطلوبة، حتى وإن كانت حساسة وخاصة. على الرغم من أن أمن المعلومات قد يكون عرضة للاختراق من خلال أدوات مثل أنظمة التجسس أو الفيروسات، إلا أن الأمن السيبراني يعمل كنظام متكامل لحماية الأجهزة الإلكترونية، بما في ذلك أجهزة الراوتر، من أي تهديدات أو فيروسات. كما يقوم بتنبيه المستخدم لاتخاذ الإجراءات المناسبة لمنع سرقة البيانات التي قد تُستخدم في قضايا الابتزاز (١٤).

٢-٢-٢- تمييز الامن السيبراني عما يرتبط به من المفاهيم

توجد العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

١- الفضاء السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام"ANSSI" بانه:" فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، وهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين".

---

(١٠) علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، الطبعة الثالثة، دار المناهج للتوزيع والنشر، الاردن، ٢٠٠٠,ص٢٩٣.

(١١)وهي اختصار لـ *Central Intelligence Agency، وتأسست وكالة المخابرات المركزية (CIA) في عام ١٩٤٧م، منذ نشأتها، أصبحت الوكالة جزءًا أساسيًا من الجهاز الاستخباراتي الأمريكي، حيث تعمل في فترات السلم والحرب على حد سواء. وقد تم الاعتراف رسميًا بدور الوكالة باعتبارها أداة ضرورية لتقديم الخدمات الاستخبارية في عالم يتسم بالاضطرابات السياسية والتقلبات المستمرة. ينظر: مجاهد صلاح، المخابرات المركزية الامريكية (CIA)، متاح على الموقع الالكتروني: https://pulpit.alwatanvoice.com/articles/ تاريخ اخر زيارة ٢٠٢٥/٢/٢٣.

(١٢) مني عبد الله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، بحث منشور في مجلة كلية التربية، جامعة المنصورة، العدد (١١١)، يوليو ٢٠٢٠,ص١١.

(١٣) خالد ظاهر عبد الله جابر السهيل المطيري، المصدر السابق، ص٩٩٩.

(١٤) ما هو الفرق بين أمن المعلومات والأمن السيبراني, مقال منشور على الموقع الالكتروني https://cyberone.co/ تاريخ الزيارة للموقع ٢٠٢٤/١١/٢١.

٢- الهجمات السيبرانية: تعرف بأنها: "فعلا يقوض من قدرات ووظائف شبكة الحاسوب لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام".
٣- الردع السيبراني: يعرف بأنه: "حماية الأصول الوطنية في الفضاء والأصول الداعمة للعمليات الفضائية من أي أنشطة ضارة".
٤- الجريمة السيبرانية: تعرف بانها: "مجموعة الأفعال والأعمال غير القانونية التي تُنفذ باستخدام الأجهزة الإلكترونية أو عبر شبكة الإنترنت أو التي يتم بث محتوياتها من خلالها."

بناءً على ما تم ذكره، يمكن القول إن الأمن السيبراني يتكون من مجموعة من الآليات والإجراءات والوسائل الوقائية والعلاجية التي تهدف إلى حماية البرمجيات وأجهزة الحاسوب، وكذلك الفضاء السيبراني بشكل عام، من الهجمات والاختراقات والتهديدات التي قد تؤثر على الأمن القومي للدول. الأمن السيبراني أيضا هو مجموعة من الممارسات والتقنيات التي تهدف إلى حماية شبكات الكمبيوتر والأنظمة الرقمية من الهجمات والتهديدات السيبرانية التي قد تؤدي إلى الوصول غير المصرح به أو التلاعب بالمعلومات. يعتمد الأمن السيبراني على أدوات مثل جدران الحماية، وأنظمة اكتشاف التسلل، والتشفير لضمان سرية البيانات وسلامتها، بالإضافة إلى تأمين بروتوكولات الاتصال مثل" HTTPS وVPN". كما يتعامل مع تصحيح الثغرات الأمنية والتحديثات المستمرة للحفاظ على حماية الأنظمة. أما الجرائم الإلكترونية فهي أفعال غير قانونية تُرتكب عبر الإنترنت أو باستخدام الأنظمة الرقمية، بهدف انتهاك سرية المعلومات أو تدمير أو تغيير البيانات بشكل غير مصرح به. تشمل هذه الجرائم مثل الاحتيال الإلكتروني، وسرقة الهوية، والهجمات على الشبكات (مثل هجمات حجب الخدمة DDoS)، وعمليات الاختراق والتجسس الإلكتروني.

٣- الاليات الدولية والوطنية في تحقيق الامن السيبراني

لم تعد التهديدات الأمنية مقتصرة على قوة السلاح فقط، بل أصبحت تشمل وسائل إجرامية حديثة تعتمد على التقنيات المتطورة. فقد شهد العالم تحولات كبيرة، حيث أصبحت الاتصالات أسهل بفضل ثورة تكنولوجيا المعلومات، مما حول العالم إلى قرية صغيرة. هذه التحولات تقتضي ضرورة البحث في كيفية مواجهة هذه الجرائم الإلكترونية، مما استدعى الحاجة إلى إطار قانوني ينظم تلك العلاقات. وقد دفع ذلك الأمم المتحدة إلى تخصيص إحدى هيئاتها لمتابعة هذا الموضوع، وتسابقت الدول لحماية فضاءها السيبراني من الهجمات، نظراً لما تشكله من تهديدات قد تؤدي إلى انهيار اقتصادي، كما حدث في بعض الدول بسبب عمليات القرصنة المنظمة على بنيتها السيبرانية أو تهديدات أمنية قد تؤدي إلى انهيار سياسي وأخلاقي واجتماعي. في هذا السياق، سنستعرض في هذا المبحث الاليات الدولية والوطنية المبذولة لتحقيق الأمن السيبراني. في المطلب الأول، سنتناول الاليات الدولية في هذا المجال، وفي المطلب الثاني، سنتطرق إلى الاليات الوطنية لتحقيق الأمن السيبراني.

٣-١- الاليات الدولية لتحقيق الامن السيبراني

أسفرت الاليات الدولية الرامية إلى تنظيم التفاعلات وسلوك الفاعلين في الفضاء السيبراني، في إطار التنظيمات الدولية القائمة، عن إبرام عدد من الاتفاقات الدولية. تشمل هذه الاتفاقات ما يتعلق بوضع وصياغة الخطط والاستراتيجيات الوطنية، بالإضافة إلى تقديم الدعم التقني والفني. كما تشمل توفير القوى البشرية لتدريب الكوادر المختصة، فضلاً عن دعم تفعيل آلية المحاسبة والعقاب، كما هو الحال في المنظمة الدولية للشرطة الجنائية (الإنتربول).

٣-١-١- الدور الاممي لتحقيق الامن السيبراني:

لقد لعبت الأمم المتحدة دورًا بارزًا في تنظيم وتطوير إطار عمل لمكافحة الجرائم السيبرانية، من خلال وضع قواعد موضوعية وإجرائية، بالإضافة إلى تنظيم مؤتمرات وقمم دولية وتفعيل جهود بعض هيئاتها وأجهزتها. من بين القواعد الموضوعية التي تم تبنيها، تم تحديد قائمة بالأفعال التي يجب تجريمها باعتبارها جرائم سيبرانية، مع تحديثها بشكل دوري. تشمل هذه الأفعال: الاحتيال أو الغش المرتبط بالحواسيب، التزوير الذي يطال برامج الكمبيوتر أو التزوير المعلوماتي، التخريب وإتلاف الحاسوب، الدخول غير المصرح به، واعتراض البيانات بشكل غير قانوني. أما فيما يتعلق بالقواعد الإجرائية، فقد تم التأكيد على ضرورة تحديد السلطات المختصة بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات. كما تم التأكيد على أهمية التعاون الفعال بين الدول لتنسيق الجهود القضائية في معالجة الجرائم السيبرانية، مع تمكين السلطات العامة من اعتراض الاتصالات داخل الفضاء المعلوماتي واستخدام الأدلة المتاحة. كما تم إدخال تعديلات تشريعية عند الحاجة لتواكب طبيعة الجرائم السيبرانية في القوانين الوطنية، مع مراعاة القواعد الخاصة بالإثبات الإلكتروني من حيث مصداقية الأدلة وما قد يترتب عليها من تحديات عند تطبيقها ([١٥]).

(١٥) هبه جمال الدين،الأمن السيبراني والتحول في النظام الدولي, بحث منشور في مجلة كلية الاقتصاد والعلوم السياسية/ جامعة القاهرة, المجلد الرابع والعشرون ، العدد الأول ، يناير ٢٠٢٣,ص٢٠٦.

انبثقت من منظمة الأمم المتحدة عدة مؤتمرات وقمم دولية، حيث توصل المؤتمر الثامن الذي انعقد في هافانا عام ١٩٩٠ إلى إصدار قانون خاص بالجرائم السيبرانية. من بين أهم التشريعات النموذجية لمكافحة هذه الجرائم هي اتفاقية بودابست التي أُصدرت عام ٢٠٠١ عن مجلس أوروبا، والتي تُعد نموذجًا يمكن أن يُسترشد به من قبل التشريعات الوطنية وقد الزمت الاتفاقية الدول الأطراف باتخاذ كافة التدابير التشريعية وغيرها من التدابير لتجريم الأفعال التاليه:" أ- ما اذا ارتكب عمدا اتلاف بيانات حاسوبية، حذفها، افسادها،تعديلها او تدميرها. ب- يجوز لدولة طرف ان تحتفظ بحقها في ان تستلزم ان تتسبب الأفعال المشار اليها في الفقرة أ في ضرر جسيم"([١٦]).

كما أصدرت الجمعية العامة للأمم المتحدة في ديسمبر ٢٠٠٢ القرار رقم (٢٣٩/٥٣) الذي يدعو إلى إنشاء اتفاقية عالمية للأمن السيبراني، وفي قرار آخر، قرار الجمعية العامة رقم ٢٣٩/ ٥٧ في٣١ يناير٢٠٠٣، دعت الجمعية الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني، وفي القرار رقم ١٩٩ / ٥٨ في ٣٠ يناير في عام ٢٠٠٤، أصدرت الأمم المتحدة قرارًا بشأن "إنشاء ثقافة عالمية للأمن السيبراني"، الذي يدعو الدول الأعضاء إلى تعزيز التعاون وتعميق ثقافة الأمن السيبراني. كما أكد مؤتمر الأمم المتحدة الثالث عشر لمنع "الجريمة والعدالة الجنائية"، الذي عُقد في الدوحة في ١٤ أبريل ٢٠١٥، على أهمية مكافحة الجرائم الإلكترونية. ولم تقتصر جهود الأمم المتحدة على ذلك، بل تواصلت من خلال تنظيم المؤتمرات وإبرام المعاهدات بهدف حماية الحياة الشخصية للأفراد وحقوقهم الفكرية في مواجهة تحديات التكنولوجيا. كما تسعى إلى التنسيق وتعزيز التعاون بين دول المجتمع الدولي لاتخاذ الإجراءات اللازمة للحد من الجرائم الإلكترونية بشكل عام ([١٧]).

كما قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية ففي أبريل من عام ٢٠١٠، في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات التي تضمنت إنشاء فريق خبراء حكومي دولي لدراسة مشكلة الجريمة السيبرانية وسبل الاستجابة الدولية لها. كما لعبت الأمم المتحدة دورًا مهمًا من خلال المجلس الاقتصادي والاجتماعي التابع لها، حيث افتتحت دورته لعام ٢٠١٠ بجلسة إعلامية تناولت التحديات التي يطرحها الأمن السيبراني، بالإضافة إلى التهديدات والفرص التي يوفرها استخدام الإنترنت الذي يشهد توسعًا مستمرًا. وقد اهتمت الأمم المتحدة بالبناء المؤسسي، فأنشأت كيانات مثل الشراكة التعددية ضد التهديدات السيبرانية "Impact" في عام ٢٠٠٩، وهي أول منظمة تدعمها الأمم المتحدة بهدف تعزيز التحالف لدعم الأمن السيبراني([١٨]). في عام ٢٠١٥، تم وضع معايير محددة لمواجهة الهجمات السيبرانية، وفي عام ٢٠٢١ تم الاتفاق عليها بالإجماع من قبل جميع أعضاء الأمم المتحدة. تهدف هذه المعايير إلى وضع إطار سياسي ملزم لجميع الدول التي تستخدم الفضاء الإلكتروني. ومن أبرز هذه المعايير، تعهد الدول بمنع استخدام شبكات الإنترنت في الأنشطة التي تهدد أو تضر بالسلم والأمن الدوليين، وكذلك عدم السماح عن عمد باستخدام أراضيها في أعمال غير مشروعة.

اما بالنسبة لمجلس الامن في القرار رقم (٢٣٤١) لعام ٢٠١٧، دعا الأعضاء إلى تعزيز وبناء الشراكات الوطنية والإقليمية والدولية مع الأطراف المعنية في القطاعين العام والخاص، بهدف تبادل المعلومات والخبرات من أجل الوقاية من الهجمات الإرهابية على البنى التحتية الحيوية، وحمايتها، والتخفيف من آثارها، والتحقيق فيها، ومواجهتها، والتعافي من الأضرار الناتجة عنها. ومن بين الوسائل المقترحة لتحقيق ذلك: التدريب المشترك، وإنشاء واستخدام شبكات مناسبة للاتصال والإنذار في حالات الطوارئ.

٣-١-٢- الدور الاقليمي لتحقيق الامن السيبراني:

تبلورت الاليات الإقليمية في مجال الأمن السيبراني عبر إنشاء منظمة حلف شمال الأطلسي (الناتو) لهيئات معنية بإدارة الدفاع السيبراني، مثل فريق الاستجابة للحوادث السيبرانية الذي يضمن إرسال فرق الدعم السريع إلى الدول الأعضاء، بالإضافة إلى مركز التميز المخصص للتعاون في الدفاع السيبراني. من جهة أخرى، توصل المجلس الأوروبي إلى اتفاقية "بودابست بشأن الجرائم السيبرانية"، التي تتناول بعض الجرائم السيبرانية وتوفر أحكامًا قانونية يمكن أن تتبناها الدول وتعدلها لتناسب احتياجاتها. ورغم أن الاتفاقية تعالج قضايا مثل القرصنة واعتراض الاتصالات، فإنها لا تشمل بعض الهجمات السيبرانية الأكثر تهديدًا مثل التجسس على البيانات وأعمال التخريب. وتواجه الاتفاقية قيودًا في قوتها الإلزامية بسبب محاولة الحفاظ على التوافق مع التشريعات الوطنية المختلفة. منذ فتح باب التوقيع في نوفمبر ٢٠٠١، صدقت ثلاثون دولة فقط على المعاهدة، بما في ذلك دولة واحدة خارج أوروبا. كما قام الاتحاد الدولي للاتصالات باتخاذ خطوات لمعالجة مسائل الأمن السيبراني في الشبكات الذكية من خلال إنشاء فريق متخصص يعنى بجمع وتوثيق المعلومات اللازمة لإعداد توصيات تدعم الأمن السيبراني في هذا المجال وتعزز فعالية التصدي للهجمات السيبرانية([١٩]).

---

(١٦) ينظر المادة (٤) من الاتفاقية المتعلقة بالجريمة الالكترونية (بوداست) لعام ٢٠٠١.

(١٧) منير محمد الجنبيهي و محمود محمد التنبيهي، تزوير التوقيع الالكتروني،دار الفكر الجامعي، الإسكندرية، ٢٠٠٦،ص١١١.

(١٨) هبه جمال الدين،الأمن السيبراني والتحول في النظام الدولي ، المصدر السابق، ص٢٠٧.

(١٩) هبه جمال الدين ، مصدر سابق، ص٢٠٧.

وعلى الصعيد العربي، تم بذل جهود كبيرة في مواجهة الجرائم السيبرانية والإلكترونية، ففي الاطار التشريعي اسفرت الاليات المتخذة علي الصعيد العربي عن إبرام اتفاقية عربية لمكافحة جرائم تقنية المعلومات، والتي تم التوصل إليها خلال الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب في مقر الأمانة العامة لجامعة الدول العربية عام ٢٠١٠. تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مكافحة الجرائم السيبرانية وتقنية المعلومات التي تهدد الأمن والمصالح الوطنية وسلامة المجتمعات. كما تسعى إلى تلبية الحاجة إلى تبني سياسة جنائية موحدة لحماية المجتمع العربي من هذه الجرائم، وذلك استناداً إلى الالتزام بالمعاهدات والمواثيق العربية والدولية ذات الصلة ([٢٠]). وقد نصت الاتفاقية في المادة الأولى منها على أن: "تهدف هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات ، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربة ومصالحها وسلامة مجتمعاتها وأفرادها". كما ان الاتفاقية في المادة (٢٥) نصت على الزام جميع الدول الأطراف في الاتفاقية، مع مراعاة قوانينها الداخلية، بترتيب مسؤولية جزائية بحق الأشخاص الاعتبارية عن أي جريمة يرتكبها من يمثلها باسمها أو لصالحها، دون الإخلال بفرض العقوبة على مرتكب الجريمة شخصياً.

بناءً على ما سبق، يتضح أن هناك اهتمامًا متزايدًا من قبل المجتمع الدولي ووعيًا متناميًا بأهمية اتخاذ التدابير الوقائية والعلاجية في مواجهة الجرائم السيبرانية. وقد تجسد هذا الاهتمام في القرارات التي اتخذتها الأمم المتحدة ومجلس الأمن الدولي، والتي تهدف إلى تعزيز الأمن السيبراني على الصعيدين العالمي والإقليمي. بالإضافة إلى ذلك، وكذلك تعززت الاليات الدولية لتحقيق الامن السيبراني في اطار تشريعي تمثل في ظهور العديد من الاتفاقيات الدولية والإقليمية التي تعكس الجهود المستمرة للمجتمع الدولي في التصدي لهذه الجرائم. وتستهدف هذه الاتفاقيات حماية الأفراد والمؤسسات من التهديدات المتزايدة والمتطورة التي تمثلها الجرائم الإلكترونية، مما يعكس إرادة المجتمع الدولي في الحفاظ على الأمن الرقمي وتعزيز التعاون بين الدول لمكافحة هذه الظاهرة العالمية.

٣-٢- الاليات الوطنية لتحقيق الامن السيبراني

أصبح الأمن السيبراني في الوقت الحالي من العوامل الأساسية التي تؤثر في استقرار أي دولة، بما في ذلك العراق، ويعد من العناصر الحاسمة في تحقيق النمو والازدهار. وبحسب " المؤشر الوطني للامن السيبراني"(NCSI) حقق العراق درجة (١٠.٠٠) مما يضعها في المرتبة (٦٧) عالميا ، وهذا الترتيب يشير الى حاجة العراق لتعزير الجهود الوطنية في مجال الامن السيبراني. وتواجه الحكومة والمؤسسات العراقية تحديات كبيرة في هذا المجال، ويرجع ذلك إلى عدة أسباب تؤثر على فعالية النظام السيبراني في البلاد. من أبرز هذه التحديات هو نقص الوعي السيبراني لدى المواطنين والمؤسسات، حيث لا يزال الوعي بأهمية الأمن السيبراني ضعيفًا في العراق رغم ضرورتها. كما أن التشريعات المتعلقة بالأمن السيبراني، رغم وجود بعض المبادرات القانونية، تظل غير كافية وغير متكاملة، مما يستدعي تطوير تشريعات أكثر صرامة وشمولية لحماية النظام السيبراني والتصدي للجرائم الإلكترونية. ويسعى العراق الى تعزيز الامن السيبراني وحمايته من خلال عدة اليات وطنية ، وتمثلت الاليات الوطنية لتحقيق الامن السيبراني بالاتي:

٣-٢-١- الاستراتيجية الوطنية للامن السيبراني العراقي لعام ٢٠١٧ ([٢١]).

اشارت الاستراتيجية الى اهدافها في الفقرة (٣و٣) ومن هذه الاهداف ما يلي:

- "تشريعات شاملة لمكافحة الجريمة السيبرانية والتدابير المضادة للتهديد السيبراني التي يمكن اعتمادها على الصعيد الوطني، الإقليمية والعالمية ذات الصلة في سياق تأمين الفضاء السيبراني للبلاد".
- "توفير التدابير التي تحمي البنية التحتية الحيوية للمعلومات، فضلا عن الحد من مواطن الضعف والثغرات الوطنية من خلال إطار ضمان الأمن السيبراني".
- "وضع الية فعالة للاستجابة لحالات الطوارئ في الحاسوب".
- "العمل على تحسين قدرة وتطوير فريق الاستجابة لحالات الطوارئ في الحاسوب العراقي".
- "وضع آلية موثوقة لإشراك أصحاب المصلح المتعددين والوطنيين والدوليين من أجل التصدي بشكل جماعي

(٢٠) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الديباجة، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية, ٢٠١٠.
(٢١) هي استراتيجية الاستعداد الوطني لتوفير تدابير متماسكة وإجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع إنترنت موثوق به. ينظر: الاستراتيجية الوطنية للامن السيبراني, ص٢.

للتهديدات السيبرانية".

- "الردع وحماية الحكومة من جميع أشكال الهجمات السيبرانية".
- "تنسيق مبادرة الأمن السيبراني على جميع مستويات الحكومة في البلاد".

٣-٢-٢- الاطار التشريعي لتحقيق الامن السيبراني.

١- نص قانون العقوبات العراقي رقم (١١١) لسنة١٩٦٩ ([٢٢])، على تحريم الاعتداء على وسائل الاتصال السلكي واللاسلكي فيه وانه لم يعالج الجريمة الحاسوبية، ولكن جاء بنص عام.

نص القانون رقم (٣١) لسنة ٢٠١٣([٢٣])، لتصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على ان:" تهدف هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء اخطار هذه الجرائم حفاظا على امن الدول العربية ومصالحها وسلامة مجتمعاتها وافرادها". وقد نصت المادة (٢١٦) على تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال :أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمستخدمين والمستفيدين .ب- الحصول على معلومات حكومية سرية. من الاتفاقية كما نصت المادة (٢١) من القانون على:" تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات".

٣-٢-٣- الاليات الاخرى لتحقيق الامن السيبراني.

١- اقرار وثيقة سياسات ومعايير امن المعلومات والبيانات، والتي تهدف الى وضع اطر العمل والسياسات والمعايير وتحديد الادوار والمسؤوليات داخل المؤسسة.

٢- موافقة المجلس الوزاري للأمن الوطني على تشكيل الفريق الوطني للاستجابة للحوادث والتهديدات السيبرانية، الذي يعد فريقًا وطنيًا مشتركًا متخصصًا في مجال الأمن السيبراني، ويختص بالاستجابة للحوادث السيبرانية وحماية البنية التحتية للإنترنت. كما يعمل على نشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الإنترنت. يتولى الفريق مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في الفضاء السيبراني العراقي، ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في تعزيز أمنها وحماية خدماتها في الفضاء السيبران ([٢٤]).

٣- تأسيس مركز الأمن السيبراني في وزارة الداخلية بتاريخ ٤ ديسمبر ٢٠٢٢.يُعد المركز جهة أمنية متخصصة في مجال الأمن السيبراني، ويرتبط بمكتب معالي السيد الوزير. ويهدف إلى تعزيز جهود وزارة الداخلية في بناء منظومة متكاملة وفعالة لحماية الفضاء السيبراني. كما يسعى إلى تطوير وتنظيم آليات الحماية لمواجهة التهديدات السيبرانية بكفاءة وفعالية، بما يضمن استمرارية العمل، ويحافظ على الأمن الوطني، وسلامة بيانات ومعلومات المؤسسات والأفراد[٢٥].

بناء على ماسبق يتضح للباحث انه على الرغم من وجود الاستراتيجية الوطنية للأمن السيبراني العراقي لعام ٢٠١٧ وبعض النصوص التشريعية التي تهدف إلى تعزيز الأمن السيبراني، إلا أنها تظل غير كافية وغير شاملة. يحتاج العراق إلى تشريعات أكثر صرامة وتكاملًا لحماية النظام السيبراني، فضلاً عن ضرورة سن قانون خاص بالجرائم المعلوماتية فضلا عن وجود قصور في نشر الوعي في مجال حماية الخصوصية والحماية الذاتية للأفراد والمؤسسات على الإنترنت.

٤- الخاتمة

إن تحقيق الأمن السيبراني يعكس بشكل إيجابي استقرار الدولة وتطورها في العصر الرقمي المتقدم، حيث يعد أمرًا أساسيًا في عالمنا المعاصر. ولتحقيق هذا الهدف وحمايته، يتطلب الأمر تكاتف جهود الحكومات والمؤسسات والمواطنين. بالإضافة إلى ذلك، يتعين بناء

(٢٢) ينظر: المادة (٣٦٣) من قانون العقوبات العراقي رقم (١١) لسنة ١٩٦٩.

(٢٣) ينظر المادة (١) من قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (١٣) لسنة ٢٠١٣.

(٢٤) **انصر سفاح كريم,** الحروب الإلكترونية وأثرها على الامن القومي, مركز النهرين للدراسات الاستراتيجية, متاح على الموقع الالكتروني https://www.alnahrain.iq/post/1031 تاريخ اخر زيارة ٢٠٢٤/٥/٣.

(٢٥) مركز الامن السيبراني، متاح على الموقع الالكتروني ، https://moi.gov.iq. تاريخ اخر زيارة ٢٠٢٥/٢/٢٣.

منظومة سيبرانية متكاملة مع الدول المجاورة للعراق، وتعزيز تبادل الخبرات في هذا المجال. يجب أن يحظى الأمن السيبراني بأولوية قصوى في السياسات الوطنية. بناءً على دراستنا حول اليالت الأمم المتحدة لتحقيق الامن السيبراني واثرها في التشريعات العراقية، والتي تناولناها من مختلف الجوانب المحلية والعالمية، توصلنا إلى مجموعة من الاستنتاجات والتوصيات التي يمكن تلخيصها فيما يلي.:

٤-١- الاستنتاجات:

١- لا يوجد تعريف موحد للأمن السيبراني، ويمكن وصفه بأنه: "مجموعة من الآليات والإجراءات والأدوات التي تهدف إلى حماية البرمجيات وأجهزة الحاسوب، وكذلك الفضاء السيبراني بشكل عام، من الهجمات والاختراقات والتهديدات السيبرانية التي قد تؤثر على الأمن القومي للدول."

٢- على الرغم من عدم وجود تعريف موحد للأمن السيبراني، إلا أن هناك اتفاقًا على أهمية دوره البارز في توفير الحماية للبيانات والمعلومات الاستراتيجية للمؤسسات الحكومية والشركات، والحد من الجرائم الإلكترونية. كما يسهم في حماية خصوصية الأفراد، حيث أن اختراقها يمكن أن يهدد أمن المؤسسات والأفراد، ويؤدي إلى خسائر وأضرار تهز استقرار الأمن القومي للدول.

٣- يعد الأمن السيبراني جزءا في غاية الاهمية من عالم التكنولوجيا الحديثة، حيث يعمل على حماية الفضاء الإلكتروني والشبكات من الاختراقات والتهديدات السيبرانية.

٤- انطلقت جهود دولية تهدف إلى تنظيم التفاعلات وسلوك الكيانات الدولية الفاعلة في الفضاء السيبراني، من خلال العمل ضمن الأطر التنظيمية الدولية الحالية وإبرام اتفاقيات دولية تشمل المساعدة في وضع وصياغة الخطط والاستراتيجيات.

٥- وعلى الصعيد العربي، فقد بذلت جهود كبيرة في مكافحة الجرائم السيبرانية والإلكترونية، أسفرت عن وضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات.

٦- على الرغم من وجود الاستراتيجية الوطنية للامن السيبراني العراقي لعام ٢٠١٧, والتي تنظم الأمن السيبراني في العراق، إلا أنها لا تزال غير كافية والوعي بها لا يزال ضعيفا.

٧- تواجه الحكومة العراقية تحديات كبيرة في مجال تشريعات الأمن السيبراني، حيث توجد بعض التشريعات التي تهدف إلى تعزيز الأمن السيبراني، لكنها تظل غير كافية وغير متكاملة. لذا، يحتاج العراق إلى وضع تشريعات أكثر قوة وشمولية لضمان حماية النظام السيبراني بشكل فعال.

٤-٢- التوصيات:

١- اخذ التدابير الوقائية التي تدعم تحقيق الامن السيبراني.

٢- العمل على تعزيز الوعي السيبراني لدى المواطنين والمؤسسات كافة، فضلا عن تطوير البنية التحتية التكنولوجية وتحديثها بشكل منتظم لحماية الامن السيبراني.

٣- وضع التشريعات الصارمة والشمولية لحماية النظام السيبراني، حيث يفتقر العراق الى الان لقانون الجرائم المعلوماتية.

٤- منح الاعتبار لحضور المؤتمرات والندوات العالمية والاقليمية التي تهتم بواقع الامن السيبراني وحمايته.

٥- العمل على تثقيف مستخدمي الشبكة، وخلق روح المسؤولية لديهم في وجوب اتباع قواعد السلوك الصحيح أثناء إبحارهم في العالم الافتراضي، ومراعاة حقوق الاخرين، وعدم الاعتداء على حقوق الملكية الفكرية، وتزويد مقدمي الخدمات بمعلومات حقيقية.

٦- وضع التدابير والاجراءات العلاجية واخذ الاحتياطات والاستعداد للتعامل مع الحوادث السيبرانية، ويشمل ذلك إنشاء نسخ احتياطية للمعلومات والنظم، وتطوير خطط حماية واستعادة بعد الكوارث.

٥- المراجع

٥-١- الكتب

1 - دليل الامن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام ٢٠١٠.

2 - خالد الشايع، الامن السيبراني مفهومه وخصائصه وسياساته، دار العالمية، الطبعة الاولى, ٢٠١٨.

3 - سعيد عبد اللطيف حسن، اثبات جرائم الحاسوب والجرائم المرتكبة عبر الانترنيت، دار النهضة العربية، القاهرة، ط٤,بلا سنة طبع.
4 - علاء عبد الرزاق السالمي، تكنولوجيا المعلومات، الطبعة الثالثة، دار المناهج للتوزيع والنشر، الاردن، ٢٠٠٠.
5 - منير محمد الجنبيهي و محمود محمد التنبيهي، تزوير التوقيع الالكتروني،دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

٥-٢- المجلات والدوريات:

1 - خالد ظاهر عبد الله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي، بحث منشور في مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون، يوليو ٢٠٢٢.
2 - مني عبد الله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، بحث منشور في مجلة كلية التربية، جامعة المنصورة، العدد (١١١)، يوليو ٢٠٢٠.
3 - هبه جمال الدين ، الأمن السيبراني والتحول في النظام الدولي, بحث منشور في مجلة كلية الاقتصاد والعلوم السياسية/ جامعة القاهرة, المجلد الرابع والعشرون ، العدد الأول ، يناير ٢٠٢٣.
4 - نوري حمد خاطر، حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، بحث منشور في مجلة المنارة، العدد (٢)، كانون الثاني لعام ٢٠١٢.

٥-٣- الاتفاقيات الدولية

1 - الاتفاقية المتعلقة بالجريمة الالكترونية (بوداست) لعام ٢٠٠١.
2 - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

٥-٤- القوانين:

1 - الاستراتيجية الوطنية للامن السيبراني العراقي لعام ٢٠١٧.
2 - قانون العقوبات العراقي رقم (١١) لسنة ١٩٦٩.
3 - قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (١٣) لسنة ٢٠١٣.

٥-٥- مواقع الانترنيت:

1 - الأمن السيبراني، مقال منشور على الموقع الإلكتروني https://political-encyclopedia.org/dictionary.
2 - ما هو الفرق بين أمن المعلومات والأمن السيبراني, مقال منشور على الموقع الالكتروني https://cyberone.co/.
3 - انصر سفاح كربم, الحروب الإلكترونية وأثرها على الامن القومي, مركز النهرين للدراسات الاستراتيجية, متاح على الموقع الالكتروني https://www.alnahrain.iq/post/1031.
4 - جهاد صلاح، المخابرات المركزية الامريكية (CIA)، متاح على الموقع الاكتروني: [https://pulpit.alwatanvoice.com/articles/].
5 - مركز الامن السيبراني، متاح على الموقع الالكتروني ، https://moi.gov.iq. تاريخ اخر زيارة ٢٠٢٥/٢/٢٣.