ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

الامن السيبراني العراقي واثره في قوة الدولة

أ.م.د. ماجد صدام سالم
قسم الجغرافية، كلية التربية الاساسية، جامعة ميسان، العراق
البريد الالكتروني: magidsaddamsalim@uomisan.edu.iq

الملخص
أن القوة احدى وسائل وأدوات الدول لتحقيق اهدافها والمحافظة على مكتسباتها، يعد تحقيق الامن السيبراني من التحديات الامنية المعاصرة التي تمس قوة الدولة السياسية والاقتصادية في العراق، من خلال زيادة الوعي بالمخاطر السيبرانية المتحققة، لان من يمتلك آليات توظيف القوة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في اداء الفاعلين المستخدمين لهذه البيئة، فكان لثورة المعلومات والاتصالات انعكاساتها في ربط المصالح القومية للدول بالبنى التحتية الحيوية لها، والسعي في إقامة المراكز اللازمة التي يمكن الاستفادة منها في التصدي لما يقع من حوادث لاختراق الامن العراقي، ويشكل كذلك تقييم الخطر، وتنفيذ تدابير لتخفيف الأثر، وإدارة النتائج جزءاً من أي برنامج وطني للأمن السيبراني. في المساعدة على حماية سياسة واقتصاد الدولة من التخريب عن طريق المساهمة في استمرارية التخطيط عبر القطاعات المختلفة.

الكلمات المفتاحية: الامن السيبراني، الاستراتيجية، الامن الوطني، الفضاء السيبراني.

Iraqi Cyber Security and its Impact on State Power

Dr. Majid Saddam Salim
Geography Department, College of Basic Education, University of Misan, Iraq
Email: magidsaddamsalim@uomisan.edu.iq

ABSTRACT
Power is one of the means and tools of countries to achieve their goals and preserve their achievements. Achieving cyber security is one of the contemporary security challenges affecting the power of the political and economic State in Iraq. by increasing awareness of cyber risks, because those who have the mechanisms to employ cyber power become more able to achieve their goals and influence the performance of actors using this environment The information and communication revolution has had its consequences in linking the national interests of States to critical infrastructure and in seeking to establish required centers that could be used to confront breaching incidents of Iraqi security, Risk assessment, implementation of mitigation measures and results management are also part of any national cyber security program. To help protect the State's policy and economy from sabotage by contributing to the continuity of planning across different sectors.
Keywords: cyber security ,Strategy, national security, cyber space.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

المقدمة:

كان لثورة المعلومات الهائلة وظهور الانترنيت في أرجاء العالم بداية ظهور العصر السيبراني، من خلال خلق بيئة جديدة تعرف ب الفضاء السيبراني (Cyber space) اضافة الى الفضاء الارضي والبحري والجوي، والفضاء السيبراني اصبح يؤثر في النظام الدولي خاصة مع بروز أشكال جديدة من قوة الدولة ومنها القوة السيبرانية التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى المحلي والدولي، ما جعل الفضاء السيبراني مجالا جديدا للصراع بين الدول. فقد أحدثت تكنولوجيا المعلومات والاتصالات بذلك ثورة شاملة في جميع نواحي الحياة، فعلى المستوى الاجتماعي كان لها الاثر الكبير على سلوك الافراد والمجتمع، وانتشار حالات التواصل بين مجموعات بشرية مختلفة عن طريق وسائل التواصل الاجتماعي عبر الاجهزة الحديثة من الموبايل والحواسيب. وعلى المستوى الاقتصادي ساعدت التكنولوجيا الحديثة على الانتقال السريع نحو الاقتصاد الرقمي من خلال تحقيق نجاح كبير في ادارة الاعمال بالاضافة الى تزايد استخدام الابتكارات التكنولوجية في قطاعات اقتصادية حيوية ومنها الطاقة والطاقة النظيفة والسياحة والخدمات المصرفية والمالية، في مقابل ذلك تزايدت المخاطر والجرائم، كلما زاد استخدام تكنولوجيا المعلومات والاتصالات من خلال سرقة الاموال والنصب والاحتيال والتخطيط لعمليات ارهابية وترويج الاشاعات والاخبار المزيفة. وعلى هذا النحو يمكن اعتبار الامن السيبراني اعلى تحديات الامن القومي للدول في العصر الحديث والتي لاتشمل فقط الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي عن طريقها دخلت التكنولوجيا فيها من تدفق المعلومات والاتصالات بمفهوم الحدود الجغرافية السياسية مما وضع سيادة الدول على الخطر خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول واختراق حاسبات الشركات والافراد. لذلك تتعامل الجغرافيا السياسية مع شبكات الاتصالات وتوزيع الكابلات البحرية ومحاور ونقاط الاتصال التي تمر عبرها حركة الإنترنت، والتلاعب المحتمل للبيانات من خلال استخدام البيانات الاجتماعية والبيانات الضخمة، والهجمات التي يمكن ان تتعرض البنية التحتية للدولة التي من خلالها قد تكون قادرة على اخضاع الدول الاخرى.

مشكلة البحث:

في عصرنا الرقمي اليوم تزايدت فيه اعداد ومخاطر التهديدات السيبرانية وتباينت اثارها وانعكاساتها في دول العالم ، وفي العراق كان الاجدر المحافظة على الامن السيبراني كباقي القطاعات الاخرى كونه يعزز قوة الدولة مقابل الهجمات المحتملة على المفاصل العسكرية والاقتصادية العراقية وفلذلك تبرز مشكلة البحث:

ماهو أثر الهجمات السيبرانية الدولية والمحلية على قوة الامن السيبراني العراقي.؟

فرضية البحث:

العراق اليوم يمر بحالة عدم استقرار في كثير من الجوانب ومنها الجانب الالكتروني، بعد القضاء على التنظيمات الارهابية التي كانت تستخدم الفضاء السيبراني في بث روح الكراهية والحقد وكذلك في استخدام التكنولوجيا الحديثة في معظم العمليات الارهابية. وستكون فرضية البحث في الاجابة على سؤال المشكلة بان :

ان مواجهة التهديدات السيبرانية لها الاثر الكبير في الحفاظ على قوة العراق السيبرانية.

اهمية البحث: يندرج موضوع البحث في الجغرافية السياسية ضمن محو الدراسات الاستراتيجية كحقل معرفي خاصة بعد التطور التقني وثورة المعلومات الكبيرة التي اجتاحت العالم واصبح كقرية صغيرة. فالمحافظة على الامن السيبراني العراقي كاحد مقومات القوة التي يمتلكها العراق مع باقي الدول الاقليمية.

اهداف البحث: من اهداف البحث هو ابراز وتوضيح المفاهيم المتعلقة بل الفضاء السيبراني للعراق وتوضيح العلاقة مابين قوة الامن السيبراني والامن القومي العراقي من مختلف الجوانب. عبر تشخيصها للواقع ورصد الابعاد والمؤشرات لتساعد في تكوين رؤية واضحة وبتالي اتخاذ القرار المناسب والمطلوب.

المبحث الاول: عناصر الامن السيبراني: (Cyber Security Elements)

الأمن السيبراني جاء من كلمتي (Cyber security)، وكلمة سيبر لاتينية الأصل ومعناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي، وهو تعبير أشمل وأعم من أمن المعلومات. لذا يمكن القول أن الأمن السيبراني هو مجموعة الوسائل التقنية والإدارية التي يتم إستخدامها لمنع الإستخدام غير مسموح به وسوء الإستغلال، واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات التي تحتويها بهدف ضمان توافر وإستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية للمواطنين. يشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلكتروني، بما في ذلك العمليات والآليات التي يتم

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

من خلالها حماية معدات الحاسب الآلكتروني والمعلومات والبيانات من أي تدخل غير مقصود أو غير مسموح به أو تغيير أو إتلاف يمكن ان يحدث. فلقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لمواجهة الحروب الإلكترونية المستقبلية.

تتعد مفاهيم الامن السيبراني فهنالك من يقوم بتوسيعها لكي تعبر عن القدرة على حماية بيانات الدولة وشبكاتها مثل تعريف (Lewis ,J,A) بأنها حماية شبكات الحاسوب والمعلومات التي تحتويها من الاختراق أو التدمير او الاضطرابات الضارة، (خليفة، الامن السيبراني الماهية والاشكاليات، 2019، صفحة 5) وهنالك مفهوم يرى انه القدرة على حماية او الدفاع عن استخدام الفضاء السيبراني من الهجمات السيبرانية، او هو فن ضمان وجود واستمرارية مجتمع المعلومات في دولة ما وضمان وحماية المعلومات والاصول والبنية التحتية الحيوية في الفضاء الالكتروني. ومن المفاهيم من يحدد اجراءات وسياسات للامن السيبراني مثل تعريف الاتحاد الدولي للاتصالات والذي يشير الى انه مجموعة الادوات والسياسات والمفاهيم الامنية والضمانات والمبادى ومناهج ادراة المخاطر والاجراءات والتدريبات وافضل الممارسات والضمانات التكنولوجية التي يمكن استخدامها لحماية البيئة السيبرانية المستخدمة والمنظمة بصورة عامة. لذلك الامن السيبراني النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج ولا تتحول الاضرار الى خسائر دائمة (الاشقر، 2017، صفحة 26).

كما يعرف الامن السيبراني كذلك بأنه عملية الحد من خطر الهجمات الضارة على برامج واجهزة الكمبيوتر والشبكات من خلال استخدام ادوات كشف الاختراقات ووقف نشاط الفيروسات، ومنع الدخول غير المسموح به، وتأكيد الهويات وتمكين الاتصالات المشفرة، وهو كذلك مجموعة من التقنيات والعمليات والممارسات لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم او الضرر او الوصول غير المسموح به من اجل ضمان السرية والنزاهة. ويتكون الامن السيبراني من عناصر رئيسية وهي:

1- القوة السيبرانية: (Cyber Power)

يعد استاذ العلاقات الدولية (Nye. S Joseph) من اهم مفكري القوة السيبرانية كشكل جديد للقوة حيث يعرف (جوزيف ناي) بانها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الالكتروني، اي انها القدرة على استخدام الفضاء الالكتروني لخلق مزايا والتاثير في الاحداث المتعلقة بالبيئات الواقعية الاخرى، (دحماني، 2018، صفحة 24) وذلك عبر أدوات الكترونية ويعرفها (دانيال كويل) بانها القدرة على استخدام الانترنيت لخلق مزايا والتاثير على الاحداث في البيئات التشغيلية كافة من خلال ادوات القوة. لقد أدت ظاهرة الفضاء الالكترونى الى تحول جزء من العالم من الطابع الطبيعي المادي الى عالم رقمى الكتروني، وأصبح الفضاء الالكتروني مجال جديد للتفاعلات الدولية سواء أكانت تفاعلات صراعية أو تعاونية، وأثر ذلك على تغير طبيعة القوة وبروز تهديدات الفضاء الالكتروني، وأثر بدوره على استراتيجيات الأمن القومى للدول، والسعى الى الاستحواذ على مصادر القوة داخل الفضاء الالكتروني لمنع تعرض بنيتها التحتية والحيوية للخطر، ومن ثم دخل المجال الالكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين فيها. وتركز عناصر القوة السيبرانية على وجود نظام متماسك يعظم من القوة المحصلة من التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وارادة الدولة وغيرها من العوامل التي تسهم في دعم امكانيات الدولة على ممارسة الاقناع عبر الفضاء السيبراني. (صفاء، 2020، صفحة 154).

وعليه يمكن القول ان القوة السيبرانية ترتكز على وجود نظام متماسك فيه تناغم بين القدرات التكنولوجية والاقتصاد والقوة العسكرية وادارة الدولة وغيره من العوامل التي تساهم في دعم امكانيات الدولة على ممارسة الاكراه والاقناع او التاثير على الدول الاخرى من خلال السيطرة على الفضاء الالكتروني، ومازاد من حالة الانكشاف الامني للدولة وذلك باعتمادها المتزايد على الفضاء الالكتروني كالبرامج الحكومة الالكترونية التي اصبحت عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وهو ما جعل المعضلة الامنية التي كان تعاني منها الدول في السابق تبرز من جديد لتكون امام معضلة امنية سيبرانية. (شلوش، 2018، صفحة 199).

2- الفضاء السيبراني: (Cyber Space)

هو بيئة تفاعلية حديثة تشمل عناصر مادية وغير مادية مكونة من مجموعة من الاجهزة الرقمية وانظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين او مستعملين وتجدر الاشارة الى ان مسألة تحديد مفهوم الامن السيبراني

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

هي مسألة نسبية تتوقف على طبيعة ادراك وفهم كل من الدول والهيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء. (زروقة، 2019، صفحة 1018)، ويعد الفضاء السيبراني نقطة الانطلاق لصياغة الاستراتيجية السيبرانية، فمن خلال الطريقة التي بها يوضع تعريف ومفهوم لهذا الفضاء تتبع وجهات النظر التي تعتمدها الاستراتيجيات الوطنية. (دانيال، 2019، صفحة 71) . وشكل (1) يوضح ترابط عناصر الامن السيبراني بمنظومة الفضاء السيبراني.

يستخدم الفضاء السيبراني كوسيلة للصراع داخل الدولة - دولة الصراع ، من بين مكوناتها على أسباب دينية أو اقتصادية أو دينية ، تساعد فضح ديناميات التفاعل الداخلي ، مما يسهل عملية الاختراق خارجية من خلال شبكات الاتصال في دعم طرف النزاع بغير قتالي . (Asmaa Khalid Jarjees Al-Tae, 2020, p. 473)

3- **الدفاع السيبراني: (Cyber Defense)**

يقصد به الدفاع الالكتروني لمجموعة القدرات النظامية التي تمتلكها القوات المسلحة او القوات الامنية الاخرى من تاثيرات الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة، وقد عرفت العقيدة الفرنسية الدفاع الالكتروني على انه مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء الالكتروني عن نظم المعلومات السرية والمهمة، بينما الاستراتيجية النمساوية فان الدفاع السيبراني يشير الى جميع التدابير اللازمة للدفاع عن الفضاء الالكتروني بالوسائل المناسبة لتحقيق الاهداف العسكرية الاستراتيجية، ويعرفه البرلمان الاوربي بانه عملية تطبيق الاجراءات الامنية من اجل الحماية من الهجمات السيبرانية والتعامل معها بما تستهدف تأمين البنية التحتية لنظم الاتصالات والسيطرة. يمكن أن تنتقل المعلومات السيبرانية أيضًا عبر الفضاء الإلكتروني لخلق قوة ناعمة من خلال الجذب مواطنين في دولة أخرى. ومن الأمثلة على ذلك حملة الدبلوماسية العامة عبر الإنترنت. ولكن يمكن أن تصبح المعلومات السيبرانية أيضًا مصدرًا للقوة الصلبة يمكنه إلحاق الضرر بالأهداف المادية في دولة آخرى. (Joseph S. Nye, 2010, p. 6)

4- **الردع السيبراني: (Cyber Deterrence)**

نتيجة لطبيعة الفضاء الالكتروني فانه من الصعوبة منع الهجمات السيبرانية بصورة كلية من الاساس نتيجة للهجمات الصفرية او الثغرات التي يتم اكتشافها حديثا او الفيروسات والاسلحة السيبرانية التي يتم تطويرها، فضلا عن صعوبة تعقب مصدر الهجمة ومعرفة الفاعل من الناحية الفنية، ولذا فان تحقيق الردع بطرقه التقليدية قد لا يتحقق في افضل الاحوال في الفضاء الالكتروني، ويثبت نجاحا فعليا كما في حالات الردع التقليدي مثل الردع النووي وقد دفع ذلك بصورة مباشرة الى اعادة تعريف الردع والبحث عن تعريف غير تقليدي يتلائم مع الطبيعة السيبرانية للعلاقات الدولية وهذا قد يتحقق من خلال تبني خطط واستراتيجيات للتعامل مع الهجمات السيبرانية في حالة حدوثها، تشمل التخفيف من حدتها وعدم تأثير البنى التحتية الحرجة والخدمات الرئيسية والمعلومات الهامة التي تشكل ركيزة للامن القومي للعراق.

فالردع السيبراني يتعلق بالقدرة على تغيير تصرفات الخصم من خلال تغيير حسابات التكلفة والعائدفهو يعكس تقييمات ذاتية ونفسية وحالة ذهنية ناجمة عن وجود تهديد موثوق به برد فعل مضاد غير مقبول ويمكن ان تنتج عنه مايسمى الردع بالرفض. (Singer, 2014, p. 55)

5- **الهجوم السيبراني: (Cyber Attack)**

هو من الافعال التي تقوض القدرات والوظائف لشبكات الحاسوب من اجل هدف قومي او سياسي، من خلال استغلال نقاط الضعف لتمكن المهاجم من خرق الانظمة والعبث بها، ان الهجوم الالكتروني له القدرة على اغلاق اجهزة الطرد المركزي النووية وانظمة الدفاع الجوية والشبكات الكهربائية التي تعد تهديداً خطيرا للامن القومي، لا ينبغي التعامل مع الهجمات السيبرانية بوصفها اعمال حرب لانها تشبه الهجمات المسلحة التي ينظمها قانون الحرب (سليمان، 2020، صفحة 249).

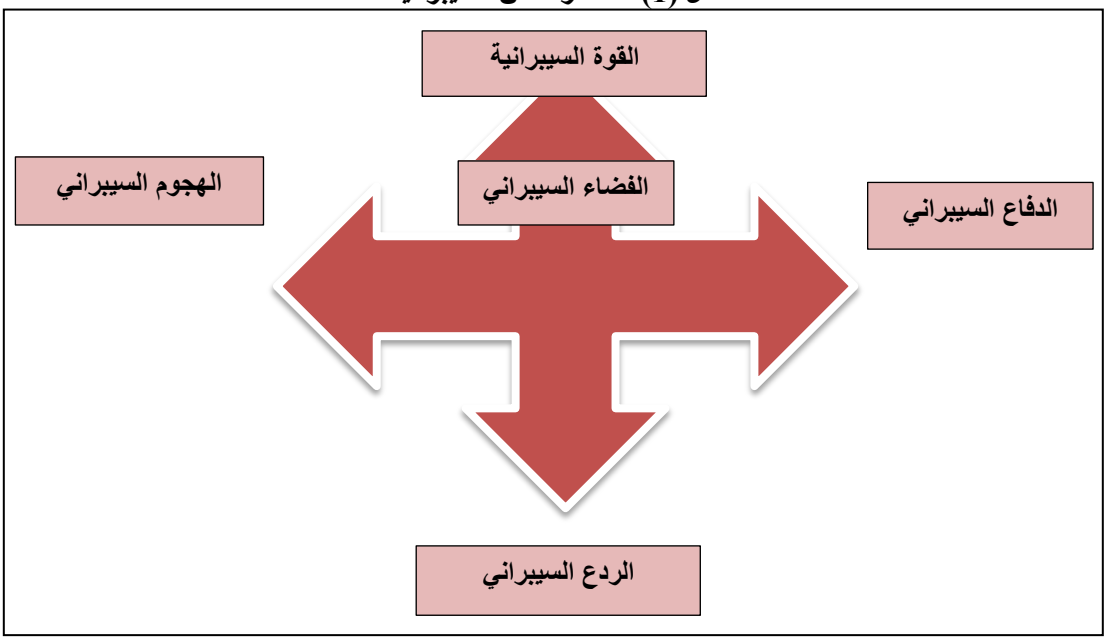
يمكن تعريف الهجوم السيبراني على أنه هجوم يشنه المهاجمون بمساعدة أكثر من جهاز كمبيوتر أو شبكة. يمكن أن تؤثر هذه الأنواع من الهجمات عن قصد على النظام كما يمكنها سرقة البيانات. يمكن تنفيذ ذلك باستخدام أجهزة الكمبيوتر المخترقة. (Noor Salah Al-Ramadan, 2021, p. 2312) ، ويمكن تقسيم الهجمات السيبرانية الى اربع فئات وهي الارهاب الالكتروني والحرب السيبرانية والجريمة السيبرانية والتجسس الالكتروني ، الا ان الارهاب السيبراني الحقيقي لا يزال نادرا ولم تكن هنالك حرب سيبرانية حقيقية ويعتقد ان المشاكل الاكثر خطورة هي الجريمة السيبرانية والتجسس الالكتروني فضلا عن اي شكل من اشكال الهجوم السيبراني هو نوع من التسلل عبر الانترنيت ولا ينبغي التقليل من خطر التطفل السيبراني. (ياسين، 2014،

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

صفحة 62) .

والجريمة السيبرانية: (Cyber Crime) هي عبارة عن مخالفة ترتكب ضد الاشخاص او الجماعات بدافع اجرامي كالدخول غير المسموح به واتلاف البيانات المخزنة في الحواسيب والعبث بها كما عرفت بانها سلوك غير مشروع يعاقب عليه القانون (سليمان، 2020، صفحة 250). هناك العديد من حالات الجرائم الإلكترونية في العراق، مثل الإنترنت الغش ، اختراق المواقع ، التداول غير المسموح به عبر الإنترنت ، الجنس الإجرامي ، اختراق الشبكة والقرصنة الإلكترونية والإرهاب السيبراني. ويجب زيادة المعرفة العامة المحلية والعالمية ومساعدة المواطنين على تجنب أن يصبحوا ضحايا للجرائم الإلكترونية. (Aboud, 2014, p. 131) .

شكل (1) عناصر الامن السيبرانية



المصدر\من عمل الباحث

المبحث الثاني: ابعاد ومؤشرات الامن السيبراني

الامن السيبراني يمكن تعريفه على أنه حماية الأنظمة والشبكات والبرامج والمواقع الجغرافية من أي مشكلة أو عائق أو هجمات إلكترونية تحول دون أداء عملها بشكل فعال وكفؤ. وتهدف الهجمات الإلكترونية عادة إلى الوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين أو مقاطعة عملها بشكل فعال. تلك العمليات لها ابعاد ومؤشرات مختلفة ويمكن ان نتعرف عليها كمايلي:

1-ابعاد الامن السيبراني:

يعتبر متغير الامن السيبراني مفهوم ذات ابعاد نسبية ومن اهمها:

البعد العسكري:

لقد كانت البدايات الاولى للانترنيت في بيئة عسكرية ب وتزايدت شكل متسارع وذلك لتنتقل في سياق اخر نحو الاوساط العلمية والاكاديمية المختلفة، وكذلك ابحاث تخدم القدرات العسكرية. وتمثل الميزة النسبية للامن السيبراني في بعده العسكري عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات والذي ينعكس ايجابا على تحقيق الاهداف العكسرية العليا. وتستخدم الدول الفضاء الالكتروني لاعتبارات الامن والقوة العسكرية بشكل جعل العديد من الدول تدخل الفضاء الالكتروني في تحقيق الرفاهية الاقتصادية والحصول على موارد الثروة والسلطة وتحقيق التفوق السياسي. (خليفة، القوة الالكترونية ، 2017، صفحة 54)

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

البعد الاجتماعي:

تعد الشبكة الدولية للمعلومات مجالا مفتوحا لجميع الاشخاص، اذ يمكن لجميع المتعاملين السيبرانيين ان يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية وهنا يجب معرفة ضرورة الاحساس باخلاقية الامن السيبراني. يفوق مستخدمي الانترنيت حاليا اكثر من 4 مليار شخص في العالم منهم 2,6 مليار يستخدمون مواقع التواصل الاجتماعي مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الافكار والخبرات الجيدة، لكن في المقابل يعرض اخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات الاختراق الخارجي قد يتسبب بتهديد السلم الاجتماعي للدولة وعليه فلابد من العمل على توعية المواطنيين بهكذا مخاطر لتحقيق الامن السيبراني في بعده الاجتماعي (زروقة، 2019، صفحة 1023).

البعد السياسي :

للدول الحق في حماية نظامها السياسي ومصالحها ، ان موازين القوى تغيرت حيث اصبح بأمكان المواطنيين ان يتحولون الى لاعبين أساسيين، واصبح بإمكانهم الاطلاع على خلفيات القرارات السياسية عبر الكم الهائل من المعلومات التي سهل عليه الوصول لها عن طريق الانترنيت ،وهنا الاشارة الى التسريبات للوثائق الحساسة مثلا والتي تثير مشاكل كبيرة وكذلك دور شبكات التواصل الاجتماعي في تنظيم الدعايات السياسية والانتخابية وتنظيم التظاهرات الافتراضية وافتعال الاحتجاجات الالكترونية. واصبح الفضاء السيبراني ملاذا للتجنيد من طرف التنظيمات الارهابية والعديد من الايدولوجيات والدعايات الدينية مما اصبح يهدد تماسك المجتمع.

البعد القانوني:

يترتب عن النشاطات الفردية والمؤسساتية والحكومية في الفضاء السيبراني، نتائج قانونية تتمثل في ايجاد القواعد القانونية التي تنظم التعاملات في الفضاء الالكتروني وحل النزاعات التي تنشأ عنها، وقد نشأت اساليب ممارساتية عديدة في استخدام تقنية المعلومات كأنشاء المدونات والتجمعات على الانترنيت والحق في حماية ملكية البرامج المعلوماتية والابلاغ عن المخالفات والجرائم السيبرانية، وهذا ما أدى الى ضرورة وجود تشريعات قانونية تتوافق مع التغيرات الحاصلة. ومما لا شك فيه ان النزاعات القانونية ستطال الاعلان الذي يرتكز الى اطياف مستخدمي الانترنيت انطلاقا من اهتماماتهم البحثية او المواقع التي يزورونها والاختراقات والتسريبات للبيانات الشخصية والمالية، سواء منها المقصودة او غير المقصودة ومسؤوليات الجهة التي تملكها او تديرها والحق في تصحيح البيانات الشخصية ومحوها وتعديلها. (الاشقر، 2017، صفحة 31). والملاحظ ان العراق بمواجهة الجريمة السيبرانية المرتكبة قد استعملت مواقع التواصل الاجتماعي وفي مقدمتها الفيس بوك وشملت هذه الجرائم الاختطاف والتهديد واختراق المعلومات الشخصية والمخدرات والاحتيال وغيرها، وتم القبض على بعض من الذين ارتكبوا جرائم الانترنيت (الشمري، 2021، صفحة 171)

البعد الاقتصادي:

يرتبط الامن السيبراني ارتباطا وثيقا بالاقتصاد فقد توسع استخدام تقنيات المعلومات والاتصالات كما بالقيمة التي تمثلها لبيانات والمعلومات المتداولة وتتيح تقنيات المعلومات تعزيز التنمية الاقتصادية للعديد من البلدان من فرص الاستخدام التي تقدمها الشركات الدولية الكبرى ولا ننسى حلول عصر المال الالكتروني ضمن بيئة تقنية متحركة كوجود المحفظة الالكترونية واصدار بطاقات الدفع الالكتروني. اذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على اصدار تطبيقات تسمح بآليات دفع آمنة وبحفظ المال في المحفظة الالكترونية . (الاشقر، 2017، صفحة 30)

2- مؤشر الامن السيبراني:

مؤشر الأمن السيبراني (GCI) يصدر عن الاتحاد الدولي للاتصالات التابع رسمياً للأمم المتحدة، ويرصد المؤشر التحسن في مستويات الوعي بأهمية الأمن السيبراني، والتدابير المتخذة لحمايته في (193) دولة من دول العالم استناداً إلى عدة مقومات عبر خمسة أركان رئيسية؛ وهي: (التدابير القانونية، والتدابير التنظيمية، والتدابير التقنية، والتدابير الرامية إلى تعزيز القدرات في مجال حماية الأمن السيبراني، وأخيراً التدابير التي تهدف إلى تعزيز التعاون). صنف المؤشر العالمي للأمن السيبراني الذي أصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة أربع دول عربية فقط في المستوى المرتفع. اقل من (25) ويرصد التقييم الذي شمل (193) دولة على مستوى العالم الممارسات والأدوات التي تستخدمها الدول لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. (UN, 2020, p. 29)

إن الرقم القياسي العالمي للأمن السيبراني يقيس مدى التزام البلدان في مجال الأمن السيبراني وفقا للدعائم الخمس

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

للبرنامج العالمي للأمن السيبراني حققت المملكة العربية السعودية إنجازًا لافتًا في مجال الأمن السيبراني، بعد حصولها على المركز الثاني عالميًا من بين 193 دولة، وتحتل المرتبة الأولى في الوطن العربي والشرق الأوسط وقارة آسيا، وفقًا للمؤشر العالمي للأمن السيبراني. وتصدرت الولايات المتحدة القائمة برصيد 100 درجة، بينما جاءت السعودية مع المملكة المتحدة في المركز الثاني بـ (99.54) لكل منهما، قفزت السعودية 11 مرتبة عن عام 2018، في التصنيف الجديد للمؤشر العالمي للأمن السيبراني، وبأكثر من 40 مرتبة منذ إطلاق رؤية 2030.
ويصدر المؤشر العالمي للأمن السيبراني عن وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات المعروفة بـ (الاتحاد الدولي للاتصالات). حققت فيه كذلك دولة الإمارات العربية المتحدة إنجازاً جديداً تجسد هذه المرة في مجال الأمن السيبراني، حيث تبوأت مؤخراً المركز الخامس عالمياً في مؤشر الأمن السيبراني (GCI) مسجلة بذلك قفزة هائلة في تصنيفها على إصدار 2020 من المؤشر، بالمقارنة مع إصدار 2019، التي نالت فيه المركز الـ 33، ومتفوقة على دول كبرى منها اليابان وكندا وفرنسا والهند. وفيما يلي ترتيب الدول العربية لعام 2020. في الجدول (1) الذي يبين ترتيب هذه الدول وموقع العراق من هذا الترتيب مع باقي الدول العربية.

جدول (1) ترتيب الدول العربية وفق مؤشر الامن السيبراني لعام 2020

الدولة	الترتيب العربي	الترتيب الدولي	النقاط
المملكة العربية السعودية	1	2	99,54
الامارات العربية المتحدة	2	5	98,06
سلطنة عمان	3	21	96,04
مصر	4	23	95,48
قطر	5	27	94,50
تونس	6	45	86,23
المغرب	7	50	82,41
البحرين	8	60	77,86
الكويت	9	65	75,05
الاردن	10	71	70,96
السودان	11	102	35,03
الجزائر	12	104	33,95
لبنان	13	109	30,44
ليبيا	14	113	28,78
الاراضي الفلسطينية	15	112	25,18
سوريا	16	126	22,14
العراق	17	129	20,71
موريتانيا	18	133	18,94
الصومال	19	137	17,25
جزر القمر	20	174	3,72
جيبوتي	21	179	1,73
اليمن	22	182	0

.Global Cybersecurity Index 2020. Measuring commitment to cybersecurity.ITU.UN.2021.p29

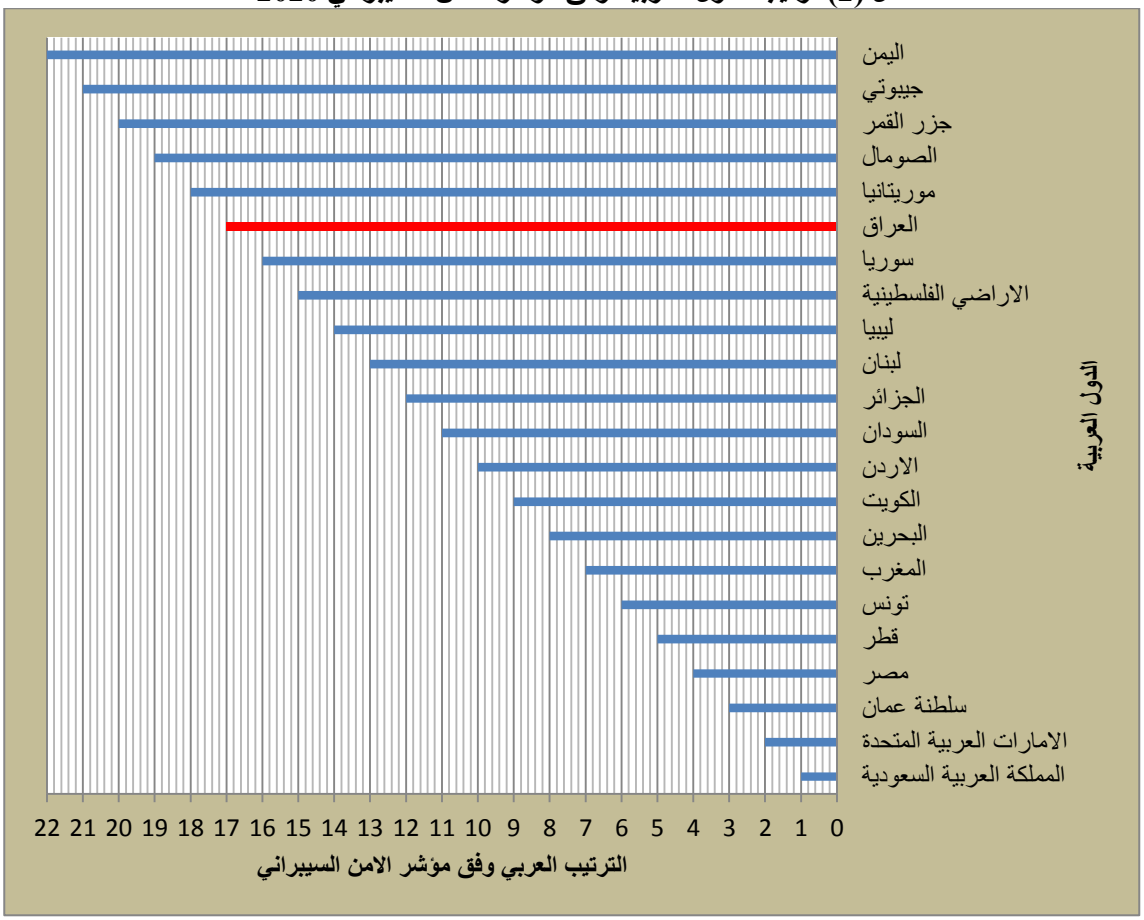
. تراجع العراق في المؤشر العالمي للأمن السيبراني (Global Cybersecurity Index) الصادر من وكالة الأمم المتحدة المختصة بتكنولوجيا المعلومات والاتصالات الاتحاد الدولي للاتصالات. اذ العراق كان في المركز

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

129 في التقرير 2020، مبيناً أن الامن السيبراني وحماية بيانات المواطنين العراقيين، جزء لا يتجزأ من الامن القومي العراقي. أن العراق تراجع عربياً ايضاً 4 مراتب، اذ حصل على المرتبة 17 متقدماً على موريتانياً، والصومال، وجزر القمر، وجيبوتي، واليمن، كما في الشكل (2) بينما تفوقت عليه بقية الدول العربية بما فيها سوريا، وفلسطين، وليبيا، ولبنان، والسودان.

وأشار التقرير، إلى أن العراق لم يقدم اجابات عن الاستبيان الذي جمعه فريق GCI والذي تضمن بعض المعلومات والبيانات، وهو الامر الذي يجب معرفته حول سبب هذا التجاهل او التهاون للجهات المسؤولة عن هذا الملف في العراق. وأنعدام وجود مؤسسات متخصصة بالأمن السيبراني في العراق، كما في الدول العربية والاقليمية، وما هو موجود عبارة عن أقسام في دوائر مختلفة تفتقد للتنسيق أو التعاون المحترف في هذا الجانب، وكل جهة منها تعمل بمفردها. وعلى العراق السعي إلى تشكيل مؤسسة أو هيئة خاصة تُعنى بقضايا الأمن السيبراني وكل ما يتعلق به في هذا الجانب، خصوصاً مع اقتراب موعد الانتخابات حيث يكون للأمن السيبراني تأثيراً مباشراً على نتائجها. يعد العراق من الدول العديدة التي تواجه تحدي الفضاء السيبراني في مختلف مجالاته ومنها المجال الامني، فحالة الضعف التي يعيشها تعقد المشكلة الاكبر، فهو لا يزال يعاني من عدم الاستقرار الداخلي بفعل الهجمات الارهابية بين الحين والاخر. في الخريطة (1) توضح التباين المكاني بين مؤشرات الامن السيبراني للدول العربية لعام 2020.

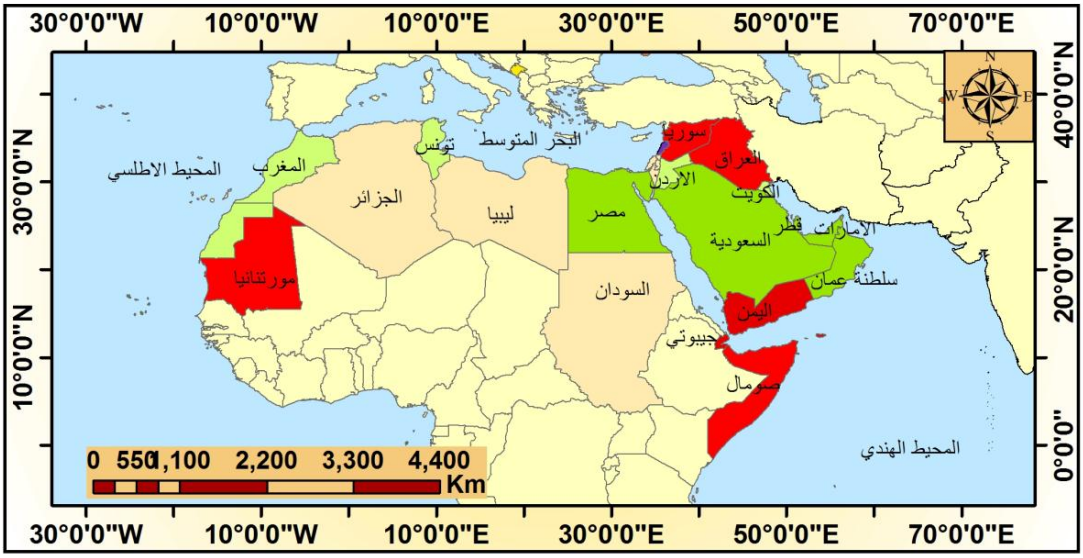
شكل (2) ترتيب الدول العربية وفق مؤشر الامن السيبراني 2020



المصدر\ بالاعتماد على جدول رقم (1)

DOI: https://doi.org/10.33193/JEAHS.18.2022.302
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

خريطة (1) التباين المكاني لمؤشر الامن السيبراني للدول العربية عام 2020



المصدر ١ بالاعتماد على برنامج Arcmap 10.2 جدول ١

لا يمتلك العراق القدرات المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني، ومع الانتقال السريع للمجتمعات من الفضاء الحقيقي الى الفضاء الافتراضي وجد العراق نفسه يدخل الى فضاء واسع وسريع الحركة، دون ان يمر بمرحلة انتقالية فالبنى المادية والبشرية لاتزال غير قادرة على التفاعل الايجابي مع تلك التحديات العديدة للفضاء السيبراني، عند البحث في الامكانات العراقية في مجال الامن السيبراني نجد انه يحتاج الى الكثير من الجهد المعرفي والاداري والقانوني والتقني لكي يكون قادر على الثاثير في مجالات الامني السيبراني من جهة ومن جهة اخرى ان يكون قادر على حماية امنه من التهديدات السيبرانية.

يعتمد مؤشر الامن السيبراني العالمي على خمس ركائز للامن عن طريق تحليل 90 مؤشر فرعي لقياس مستوى الامن السيبراني لكل دولة وهي: (خريسان، 2021، صفحة 7)

-الركيزة القانونية وتشمل على التدابير القائمة على وجود المؤسسات والاطر القانونية التي تتعامل مع الامن السيبراني والجريمة الالكترونية.

-الركيزة التقنية وتشمل التدابير القائمة على وجود المؤسسات الفنية والتعامل مع الامن السيبراني.

- الركيزة التنظيمية وتشمل على التدابير القائمة على وجود مؤسسات واستراتيجيات تنسيق السياسات لتطوير الامن السيبراني على المستوى الوطني.

-الركيزة بناء القدرات وتشمل التدابير القائمة على وجود البحث والتطوير والتعليم وبرامج التدريب والمهنين المعتمدين ووكالات القطاع العام التي تعزز بناء القدرات.

-الركيزة التعاون وتشمل التدابير القائمة على وجود شراكات وأطر تعاونية وشبكات تبادل المعلومات.

ان العراق على الرغم من التحسن الذي حدث في مؤشر عام 2018 حيث شغل المرتبة 107 عالمياً و المرتبة 13 عربياً الا انه تراجع ما يقارب 22 نقطة في مؤشر عام 2020 ليكون في المرتبة 129 عالمياً من اصل 184 دولة وبالنسبة للمرتبة 17 عربياً وبدرجة (20,71) وكان مجموع النقاط من خلال الجدول (2) الذي يوضح مجموع درجة العراق من خلال نقاط المستحصلة من فريق مؤشر الامن السيبراني.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

جدول (2) نقاط الاجراءات المتخذة من العراق وفق فريق مؤشر الامن السيبراني

الاجراءات المتخذة	الاجراءات القانونية	الاجراءات التقنية	الاجراءات التنظيمية	الاجراءات بناء القدرات	اجراءات التعاون	النتيجة
العراق	0,00	6,56	7,75	2,14	4,60	20,71

.Global Cybersecurity Index 2020. Measuring commitment to cybersecurity.ITU.UN.2021.p74

ونتيجة للحاجة الملحة لوضع اسس صحيحة للامن السيبراني العراقي في منتصف عام 2022 اعلنت وزارة التعليم العالي والبحث العلمي عن استحداث ثلاثة أقسام متخصصة في دراسة الأمن السيبراني في 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. وافتتاح 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. أن هذه الخطوة مهمة لتسهيل دراسة الأمن الرقمي وتدعيم الجهود الوطنية لحماية الفضاء السيبراني في البلاد وتطوير الخبرات المحلية. (شفق، 2022).

المبحث الثالث: علاقة الامن السيبراني بقوة الدولة

كان تصور عن مفهوم الامن بعد الحرب العالمية الثانية يقوم على الاساس النظرية الواقعية، على افتراض ان الامن يتحقق بواسطة القوة العسكرية للدول فقط، وهو كفيل بتحقيق الامن وردع مصادر التهديد القائمة انذاك من خلال علاقة القوة العسكرية للدولة وبين مدى قدرتها على حماية أمنها وضمان مصالحها، مثلا استخدام قوة الردع النووي او تلويح بها، ولهذا كانت السياسة الامنية الدولية تعتمد على القوة العسكرية لاستئصال مصدر التهديد وضمان استمرارية مصالحها.

وحتى نهاية القرن العشرين كانت الموضوعات التي سادت في الدراسات الامنية والاستراتيجية هي متعلقة بالامور العسكرية والاقتصادية وظهرت قضايا جديدة منها الامن البيئي والصحي والثقافي والالكتروني فهي قضايا تندرج في نطاق الامن غير التقليدي، يعد الامن السيبراني مجموعة الاجراءات والاطر القانونية والتنظيمية التي يتم وضعها من قبل الاجهزة الامنية للمحافظة على سرية المعلومات الالكترونية والامن السيبراني يعد جهودا مشتركة مابين القطاع العام والخاص، والجهود المحلية والدولية، بهدف حماية الفضاء السيبراني والعمل على توفير انظمة معلومات رقمية، بخصوصية عالية ، مقاومة للاختراقات الفيروسية وتتمتع بسرية عالية (العلي ، 2019، صفحة 57).

نتيجة للتقدم العلمي والتقني السريع في مجال تطوير تكنولوجيا المعلومات والاتصالات والعولمة الديناميكية ظهر بالفعل نوع جديد من التهديدات لامن الدولة والامن الدولي في العقد الاخير من القرن العشرين تهديدات تكنولوجيا المعلومات تسمى ايضا تهديدات الانترنيت انها تشكل تهديدا بسرقة او استخدام التكنولوجيا الحديثة او بيانات تكنولوجيا المعلومات والاتصالات او الحد من الجهات الفاعلة الاخرى للوصول الى بياناتهم الخاصة . وأخذت ظاهرة استخدام القوة في العلاقات الدولية تأخذ شكلا جديداً في طبيعتها ووسائلها وأدواتها واتجه الصراع الدولي بالأساس نحو المغالبة والتنافس في ساحة الإنجازات الاقتصادية والنجاحات التجارية من فوز بتعاقدات وزيادة صادرات وانتزاع الفرص وصراع حول الأفكار والإبداع والذي أصبح يترجم في شكل منتجات تكسب أسواقا وتدر أموالاً، وسعت الأمم الظافرة بكل السبل للسطو على الأسرار الاقتصادية والتقنية والعلمية والتجارية للدول الأخرى حيث اصبح للاقتصاد الرقمي الجديد دور في خلق وظائف جديدة ورفع انتاجية العامل وتوزيع جديد للدخول بين الافراد وتحفيز النمو الاقتصادي والاستثمار في المنتجات التكنولوجية والتجارة الالكترونية والتحويلات المالية وعمل البنوك واداء الحكومات الالكترونية وسهولة عملية انتقال رؤوس الاموال .

يعد الامن السيبراني أحد عناصر الامن القومي غير التقليدي وذلك لان استخدام الفضاء الالكتروني بشكل غير صحيح يمكن ان يوقع خسائر كبيرة بالطرف الثاني وان يتسبب في اختراق البيئة المعلوماتية والاتصالاتية

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

الخاصة به وهو مايسبب خسائر عسكرية واقتصادية من خلال قطع انظمة الاتصال بين الوحدات العسكرية او سرقة معلومات مهمة تتعلق باعداد العسكريين والاليات العسكرية، او من خلال التلاعب بالبيانات الاقتصادية والمالية وسرقتها او مسحها من اجهزة الحاسب الالكتروني.. وفي ميدان العلاقات الدولية أصبح امتلاك القوة السيبرانية أحد مفاتيح القوة في هذه العلاقات وبات يمثل مجالا لهيمنة الدول بعضها على بعض سواء بطريقة مباشرة او غير مباشرة وتحولت القوة العسكرية من قوة استخدام الاسلحة الى قوة الذكاء البشري. (جيجان، 2021، صفحة 38). ويمكن معرفة علاقة الامن السيبراني وقوة الدولة من خلال:.

1-فواعل القوة السيبرانية:

حدد (جوزيف س ناي) ثلاث فواعل لمن يمتلكون القوة :

-**الدول**: والتي لديها قدرة كبيرة على تفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل الحدود.

-**من غير الدول** : ويستخدمون القوة السيبرانية لاغراض هجومية بالاساس، الا ان قدرتهم على تنفيذ اي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الالكترونية واستهداف الانظمة الدفاعية. ومنهم الشركات متعددة الجنسيات والمنظمات الاجرامية والجماعات الارهابية.

-**الافراد**: الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم. (زروقة، 2019، صفحة 1019).

2-الحفاظ على الامن القومي:

ان العلاقة بين الامن السيبراني والامن القومي تزداد كلما نقل المحتوى المعلوماتي والعسكري والامني والفكري والسياسي والاجتماعي والاقتصادي وغيرهما الى الفضاء السيبراني، خاصة مع سرعة في تبني الحكومات الالكترونية والمدن الذكية في العديد من دول العالم واتساع نطاق مستخدمي الانترنيت في العالم، اذ تصبح قواعد البيانات القومية في حالة انكشاف خارجي، اضافة الى حملات الدعاية والمعلومات المضللة ونشر الشائعات او الدعوة لاعمال تحريضية او دعم المعارضة او الاقليات مما يسهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على امنها القومي. (خليفة، القوة الالكترونية ، 2017، صفحة 54). يمكن القول ان القوة السيبرانية ترتكز على وجود نظام متماسك فيه تناغم بين القدرات التكنولوجية والاقتصاد والقوة العسكرية وادارة الدولة وغيره من العوامل التي تسهم في دعم امكانيات الدولة على ممارسة الاكراه والاقناع او التاثير على الدول الاخرى من خلال السيطرة على الفضاء الالكتروني، فضلا عن ان تكلفة الحصول على القوة اصبحت مرهونة بثورة المعرفة والتطور التكنولوجي الذي مكن من ادراج فواعل جديدة في السياسات الدولية، وهو مازاد من حالة الانكشاف الامني للدولة وذلك باعتمادها المتزايد على الفضاء الالكتروني . (صالحي، 2021، صفحة 382)

وعليه فلم يقتصر اهتمام الدول بالامن السيبراني على البعد التقني وحسب بل تجاوزه الى ابعاد اخرى مثل الابعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرهما ، وهو ما عمل على دعم حقيقة ان الاستخدام غير السلمي للفضاء الالكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي اصبحت تعتمد على البنية التحتية الكونية للمعلومات. اضافة الى ان تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد اثر بدوره على سيادة الدول وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجرائم السيبرانية والجماعات الارهابية. وعليه يمكن القول ان القوة السيبرانية ترتكز على وجود نظام متماسك فيه تناغم بين القدرات التكنولوجية والاقتصاد والقوة العسكرية وادارة الدولة وغيره من العوامل التي تساهم في دعم امكانيات الدولة على ممارسة الاكراه والاقناع او التاثير على الدول الاخرى من خلال السيطرة على الفضاء الالكتروني، ومازاد من حالة الانكشاف الامني للدولة وذلك باعتمادها المتزايد على الفضاء الالكتروني كالبرامج الحكومة الالكترونية التي اصبحت عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وهو ما جعل المعضلة الامنية التي كان تعاني منها الدول في السابق تبرز من جديد لتكون امام معضلة امنية سيبرانية. (شلوش، 2018، صفحة 199).

لقد اصبحت المصالح القومية التي ترتبط بالبنية التحتية عرضة لخطر الهجوم على احدى تلك المصالح يكون سببا لحدوث عدم توازن استراتيجي ومهددا خطيرا للامن القومي، وهذا ما دفع العديد من الدول الى ادخال الامن السيبراني ضمن استراتيجيتها للامن القومي. لغرض الحفاظ على الامن السيبراني الوطني من الهجمات الخطيرة وعلى العراق تبني الاستراتيجية الوطنية للامن السيبراني وهي استراتيجية الاستعداد الوطني لايجاد تدابير واجراءات استراتيجية متماسكة لضمان امن الوجود العراقي وحمايته في الفضاء السيبراني، وحماية البنية التحتية

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

الحيوية للمعلومات، فالامن الوطني العراقي يتطلب اطارا متماسكا للامن السيبراني لضمان تهجا عاما تجاه المشهد الامني الراهن والمستقبلي. (العلي م.، 2020، صفحة 62). على الرغم من إمكانية استخدام وسائل التواصل الاجتماعي في الجرائم الإلكترونية ، لا تستطيع هذه الشركات التوقف عن استخدام وسائل التواصل الاجتماعي لأنها تلعب دورًا مهمًا في الدعاية للشركة. بدلاً من ذلك ، يجب أن يكون لديهم حلول تخطرهم بالتهديد من أجل إصلاحه قبل حدوث أي ضرر حقيقي. ومع ذلك ، يجب على الشركات فهم ذلك وإدراك أهمية تحليل المعلومات خاصة في المحادثات الاجتماعية وتقديم حلول أمنية مناسبة للابتعاد عن المخاطر. يجب على المرء أن يتعامل مع وسائل التواصل الاجتماعي باستخدام سياسات معينة وتقنيات صحيحة.

إن تطور شكل الحرب عبر التاريخ من السهام والسيوف إلى القنابل النووية والصواريخ البالستية، ينذر بالقول إن من لا يدرك جيداً تغير طبيعة وسلاح المعركة القادمة، ويسارع بالحصول عليه وتطويره، سوف ينتهي به الأمر مهزوماً تابعاً لغيره ضعيفاً بين الأمم، وسلاح الحرب القادمة سوف يكون أقوى وأبشع من القنابل النووية والهيدروجينية، فالجنود المقاتلون في هذه المعركة هم من الربوتات والدرونز، والأسلحة عبارة عن شفرات وفيروسات وديديان مبرمجة، لا يتعدى حجمها بِعض كيلوبايتات، ولكنها قادرة على إحداث تأثير يفوق في قوته الأسلحة التقليدية.

3-مكافحة الارهاب السيبراني:

الارهاب السيبراني هو الهجوم ذو دوافع سياسية او التهديد بالهجوم على اجهزة الكمبيوتر او انظمة المعلومات من اجل تدمير البنية التحتية وترهيب الحكومة او المواطنيين واجبارهم على تحقيق اهداف سياسية واجتماعية بعيدة المدى بمعنى ادق فان الارهاب السيبراني يعني استخدام الانترنيت للتواصل والدعاية والتضليل من قبل المنظمات الارهابية (المشهدي، 2019، صفحة 242). لقد أدى استخدام الإنترنت بشكل متزايد إلى تغيير لطريقة التي يعيش بها الناس وكيف تغيرت أصبح العمل ضرورة في حياتنا اليومية ، ليس فقط للترفيه ، ولكن أيضًا للتواصل مع المقربين منا. هذا يلعب دورًا حيويًا في زيادة خطر السرقة والاحتيال وسوء المعاملة. من ناحية أخرى ، لا توجد دولة أو صناعة أو حتى الأفراد في مأمن من مخاطر حوادث الأمن السيبراني وعواقبها. (Samaher Al-Janabi, 2016, p. 5) فظهور الارهاب الجديد الممتزج بتكنولوجيا الاتصال والمعلومات كشكل جديد للتهديدات الأمنية الجديدة للمجتمع الدولي وأصبح أكثر إلحاحا من أنواع الإرهاب التقليدي وذلك ينبع من خصائصه وآثاره وطبيعة أطرافه وإمكانية استخدامه في كافة الأنشطة الحساسة والأكثر تهديدا للأمن الدولي كالإرهاب النووي والبيولوجي والكيماوي والالكتروني.

اذ تعد التحديات السيبرانية واحدة من اخطر مهددات الامن الوطني العراقي ، فغياب الامن السيبراني جعل العراق دولة منكشفة استراتيجية ازاء العديد من الدول ليجسد لهم فرصة لاختراقه وتهديد امنه المعلوماتي والتحكم بكل مقدراته، وهذا جسد حافز للتنظيمات الارهابية لاختراق الامن وتوظيف مواقع التواصل الاجتماعي لنشر عقيدتهم، ناهيك عما تفرزه تلك المواقع من بث اشاعات اخذت تهدد الامن العراقي في اطار الابتزاز والسرقة الالكترونية، زد على ذلك ان ما يشهده العراق من انفتاح اعلامي كبير جعل فضاءه متاحا امام قنوات الاعلام الخارجية التي اخذت تجسد تهديدا رئيسا لامن الوطني. (العلي م.، 2020، صفحة 80) قد لا يبدو خطر الإرهاب السيبراني خطيرًا كما يبدو ، لكنه في الواقع يتعلق بحماية الأمن القومي. نظرًا لكون الإرهاب السيبراني أكثر دوافع سياسية ، فهو أكثر حرصًا على إتلاف البنية التحتية الحيوية لدولة ما والتي تتعلق بشكل غير مباشر بالتأثير على عامة الناس من حيث تعطيل البنية التحتية المالية والتجارية ، وتولي مسؤولية التحكم في السدود وحتى الوصول إلى السجلات الطبية للسكان. (Suhannia Ponnusamy, 2019, p. 3). ان معالجة قضايا الامن السيبراني على مستوى العالم يحتاج الى عمل وتعاون جماعي ودولي، ورغم الاقرار بصعوبة تحقيق مثل هذا التعاون فان الرغبة في حماية المصالح الخاصة، وامتلاك قد من الثقة بين الحكومات، قد يمهد لتعاون دولي يعمل على تحجيم التهديدات السيبرانية المستقبلية. (اسماعيل، 2020، صفحة 284)

وهنالك تراجع كبير في الامن السيبراني للعراق حسب المؤشرات الدولية ، وعند البحث عن اسباب هذا التراجع سوف نجد بأن الجهود الحكومية التي اتخذها العراق في مجال الامن السيبراني لم تستمر بل شهدت تراجع واضح وتشمل على: (خريسان، 2021، صفحة 10) .

1- ضعف أداء فريق الاستجابة للاحداث السيبرانية، وهو فريق وطني مشترك مختص بمجال الامن السيبراني والاستجابة للحوادث السيبرانية وحماية البنية التحتية للانترنيت، وقلة نشر الوعي في مجال حماية الخصوصية والحماية الذاتية للافراد والمؤسسات على الانترنيت، على الرغم انه يعمل تحت اشراف مستشارية الامن القومي

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

العراقي، ويحمل الفريق على عاتقه مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية التي تعمل في مجال الفضاء السيبراني العراقي ويقوم بتنسيق الجهود الوطنية ودعم المؤسسات في القطاعين العام والخاص في حماية نفسها وخدماتها في الفضاء السيبراني.

2- عدم تشريع قانون جرائم المعلوماتية ولم يصوت عليه بالرغم من القراءة الاولى له وتبدل نسخة لعدة مرات بطريقة تثير مخاوف على الحريات العامة.

3- قلة عدد المؤتمرات وورش العمل والندوات عن الامن السيبراني، أذ لا تزال محدودة جداً بالمقارنة مع دول الجوار .

4- قلة صرف الاموال المخصصة للامن السيبراني فهي قليلة بالمقارنة مع دول الجوار، ومنها ايران التي خصصت مليار دولار سنوياً لهذا القطاع.

5- عدم وجود بنية تحتية مادية وبشرية متكاملة في مجال الامن السيبراني ولا توجد هيئة وطنية مسؤولة عن الامن السيبراني في العراق. عدم تواجد العراق في المنتديات العالمية المعنية بالامن السيبراني

الخلاصة:

إن مفهوم القوة لايزال يمثل أحد المرتكزات الاساسية في تفسير وتحليل الظواهر السياسية بدءاً من مفهومها العسكري مروراً بمفهومها الاقتصادي وصولاً لمفهومها السيبراني، ولا تكمن القوة السيبرانية في وجود عناصرها فحسب وانما في عملية استثمارها وتوظيفها توظيفا خاصة في الجانب السياسي. يحظى الأمن السيبراني باهتمام متزايد على مستوى عالمي، وذلك بالنظر إلى خطورة التهديدات التي يمثلها انعدام الأمن الإلكتروني على الأفراد والشركات والدول، فقد أصبح الأمن السيبراني جزءاً لا يتجزأ من الأمن القومي للدول. ومن هذا المنطلق فان العراق لم يعطي اهتماماً كبيراً بهذا المجال، بل ترك الامن السيبراني للدولة والافراد في خطر من قبل الجرائم والارهاب في السنوات الماضية، ولهذا فقد حققت إنجازات ضعيفة وتمكنت من أن تكون في ذيل المؤشرات الدولية في هذا المجال، وكان آخرها في (مؤشر الأمن السيبراني) الصادر عن الاتحاد الدولي للاتصالات، التابع للأمم المتحدة، حيث أحتل العراق المرتبة السابعة عشر عربياً عام 2020 وإلى المرتبة 129 دوليا ،وبنقاط بلغت (20,71) من أصل (100 نقطة) لتكون بذلك ضمن أسوء دول العالم في تحقيق الأمن الإلكتروني. ولا شك في أن هذا ستكون له انعكاسات سلبية على مستويات مختلفة، وسيزيد من عدم الثقة بقدرات الدولة على توفير بيئة أمنة ومستقرة للأفراد والشركات، وسيسهم بالتأكيد في استبعاد الباحثين عن الاستثمار الآمن، سواء من داخل الدولة أو خارجها. مهما كان نوع القوة وطبيعتها وترتيبها حسب الادوار القائمة التي تضطلع بها وتوزيعها بين القوى الاقليمية والدولية.

النتائج:

يعد الامن السيبراني جزء من امن الدولة واهتمامها الانساني والاجتماعي، لايقل اهمية عن الامن الصحي والامن الغذائي والامن المائي، وعند تحقيق ذلك تكون الدولة قد خلقت منظومة امنية متكاملة وهادفة تشكل عماد الدولة الحضارية الحديثة يمكن استنتاج ما يأتي:

-القوة احدى ثوابت الدول، فالسيبرانية وفرت لها مجالا حركيا تتجاوز فيها الحدود الجغرافية للوصول لاهداف قد يصعب وصولها عن طريق القوة التقليدية. وهي احدى عوامل مضاعفة قوة الدول وفاعليتها

- اصبحت القوة السيبرانية حقيقة مساندة للقوة التقليدية داعمة لها في العمليات الحربية والانشطة السياسية الاقتصادية والدبلوماسية للدول والقدرة على الوصول لاهدافها المرجوة بأقل التكاليف واختصار الوقت.

أصبح الأمن السيبراني مطلبًا أساسيًا للجميع الدول المتقدمة والنامية تسعى جاهدة لتحقيق بسبب الأخطار التي تنجم عن الصراع في لذلك ، لجأت العديد من الدول إلى الفضاء الإلكتروني صياغة استراتيجيات لضمان حمايتها أمنهم السيبراني.

- القوة السيبرانية اسست رغبة للفواعل من الدول وغير الدول بالدخول الى سباق محموم للتنافس والتفوق السيبراني كما في العصر النووي سابقا.

التوصيات:

اما التوصيات فهي تتركز على ان العراق اليوم بحاجة ماسة للتكيف مع التحديات والتهديدات التي يفرضها الفضاء السيبراني في مختلف المجالات على الدولة والافراد ومنها المجال الامني ومن خلال العمل على اتباع الاتي:

1- تأسيس البنية التحتية المادية والبشرية المطلوبة للتعامل مع تحديات ومشاكل الفضاء السيبراني.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

2- تأسيس هيئة وطنية مستقلة للامن السيبراني ويمكن اعادة تفعيل فريق الاستجابة للاحداث السيبرانية وتحويله الى هيئة أمنية تنسيقية اشرافية متكاملة ، ولا يمكن ربط ها الفريق المهم بجهاز أمني بحت مثل جهاز المخابرات او غيره من الاجهزة الامنية الاخرى.

3- تأسيس كليات واقسام علمية في الجامعات العراقية المدنية والعسكرية تخص بالامن السيبراني تمنح درجات علمية في تخصص الامن السيبراني. على الرغم من تاسيسها حاليا لكن ليس بالصورة المطلوبة.

4- أنشاء مؤسسات امنية سيبرانية مثل (الشرطة السيبرانية والمخابرات السيبرانية والاستخبارات السيبرانية.. الخ) من اجل مواجهة التهديدات السيبرانية الداخلية والخارجية التي يتعرض لها العراق.

5- زيادة الوعي اعلامي وثقافي حول خطورة التهديدات السيبرانية من خلال بناء منظومة قانونية وقضائية تتعلق بالجرائم السيبرانية. ومحاسبة من يشكل تهديد على الدولة والافراد ويعرض المصالح القومية للخطر والتخريب المتعمد.

6- المشاركة في الجهود الدولية المتعلقة بالامن السيبراني مثل الاتفاقيات الدولية والمؤتمرات التي تعقد حول مخاطر التهديدات السيبرانية. والاهتمام الحكومي بالمؤشرات الدولية والاجابة الدقيقة بشفافية على الاستبيانات المعنية وفق المعطيات الامنية الممكنة.

المصادر

1-Aboud, S. J. (2014). An Overview of Cybercrime in Iraq. *The Reseach Bulletion of Jordan a c m , volume 11*, 130-136.

2-Asmaa Khalid Jarjees Al-Tae, H. A.-H.-D. (2020). Relationship of Cybersecurity and the National Security of. *A multifaceted review journal in the field of pharmacy Vol 11, Issue 12,*, 469-477.

3-Joseph S. Nye, J. (2010). *Cyber Power*. Harvard College: Belfer Center for Science and International Affairs.

4-Noor Salah Al-Ramadan, M. F. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Social Science and Humanities Journal,Vol - 05, Issue - 08,*, 2307-2323.

5-Samaher Al-Janabi, I. A.-S. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management, Vol. 15, No. 1*.

6-Singer, P. W. (2014). *Cyber Security And Cyber War*. New York.: Oxford University.

7-Suhannia Ponnusamy, G. A. (2019). *An International Study on the Risk of Cyber Terrorism.* Malaysia.: International Journal of Recent Technology and Engineering (IJRTE) Volume-7 Issue-5S,.

8-UN. (2020). *Global Cybersecurity Index Measuring commitment to cybersecurity.* Geneva: ITU.

1-احمد ياسين. (2014). *الحروب المستقبلية في القرن الحادي والعشرين*. ابو ظبي: مركز الامارات للبحوث الاستراتيجية.

2-اسراء شريف جيجان. (2021). الامن السيبراني الصيني دراسة في الدوافع والتحديات. *قضايا سياسية ،جامعة النهرين العدد 65*، 33-47.

3-اسماعيل زروقة. (2019). *الفضاء السيبراني والتحول في مفاهيم القوة والصراع*. الجزائر: مجلة العلوم القانونية والسياسية، العدد1 ، المجلد 10.

4-الموقع الالكتروني شفق. (2022). *استحداث دراسات*. بغداد: صحيفة شفق الالكترونية /https://shafaq.com/ar.

5-ايهاب خليفة. (2017). *القوة الالكترونية* . دار العربي.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.18.2022.302
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022 العدد (18) ديسمبر 2022

6-ايهاب خليفة. (2019). *الامن السيبراني الماهية والاشكاليات*. القاهرة: اوراق مصرية.
7-باسم علي خريسان. (2021). *الامن السيبراني العراقي قراءة في مؤشر الامن السيبراني العالمي 2020*. العراق: مركز البيان للدراسات والتخطيط.
8-تغريد معين حسن المشهدي. (2019). الاثر العسكري للامن السيبراني في الجغرافية السياسية. *مجلة البحوث الجغرافية العدد 30*، 239-260.
9-زياد علي العلي. (2019). *الصراع والامن الجيوسيبراني في السياسة الدولية*. عمان: دار امجد للنشر والتوزيع.
10-سليم دحماني. (2018). *اثر التهديدات السيبرانية على الامن القومي الولايات المتحدة الامريكية انموذجا*. الجزائر: جامعة بو ضياف المسيلة.
11-صالح مهدي الشمري ، زيد محمد علي اسماعيل. (2020). الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية. *قضايا سياسية، جامعة النهرين ، العدد 62*، 273-296.
12-علي فاضل سليمان. (2020). *حق الدفاع الشرعي عن الهجمات السيبرانية*. تكريت: مجلة جامعة تكريت للحقوق، العدد 4، المجلد 4.
13-فونتير ، دانيال. (2019). *الاستراتيجية السيبرانية، عالم المعرفة* . الكويت: المجلس الوطني للثقافة والفنون والاداب.
14-لبنى خميس مهدي و تغريد صفاء. (2020). أثر السيبرانية في تطور القوة. *حمورابي*، 145-161.
15-مروان سالم العلي. (2020). التحديات الاستراتيجية للامن الوطني العراقي في ظل المتغيرات الدولية. *مجلة تكريت*.
16-مصطفى ابراهيم سلمان الشمري. (2021). *الامن السيبراني واثرة على الامن الوطني العراقي*. جامعة بغداد: مجلة العلوم القانونية والسياسية.
17-منى جبور الاشقر. (2017). *السيبرانية هاجس العصر*. جامعة الدول العربي ، القاهرة: المركز العربي للبحوث القانونية والقضائية.
18-نصيرة صالحي. (2021). القوة الذكية التنافس العالمي على قوة الفضاء الالكتروني والقدرات السيبرانية. *دفاتر السياسة والقانون المجلد 13 العدد 1*، 374-385.
19-نورة شلوش. (2018). القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لامن الدولة. *مجلة بابل لدراسات الانسانية العدد 2 المجلد 8*، 199.

المصادر العربية باللغة الانكليزية:

1- Ahmed Yassin. (2014). Future wars in the twenty-first century. Abu Dhabi: Emirates Center for Strategic Research.
2- Esraa Sharif Jigan. (2021). Chinese cyber security: a study of motives and challenges. Political Issues, Al-Nahrain University, No. 65, 33-47.
3- Ismail Zarouka. (2019). Cyberspace and the shift in concepts of power and conflict. Algeria: Journal of Legal and Political Sciences, Issue 1, Volume 10.
4- Shafaq website. (2022). Create studies. Baghdad: Shafaq electronic newspaper, https://shafaq.com/ar/.
5- Ehab Khalifa. (2017). electronic force. Arab dar.
6- Ehab Khalifa. (2019). Cyber security, its essence and problems. Cairo: Egyptian Papers.
7- Biaism Ali Khreisan. (2021). Iraqi cybersecurity, a reading of the global cybersecurity index 2020. Iraq: Al-Bayan Center for Studies and Planning.
8- Taghrid Moein Hassan Al-Mashhadi. (2019). The military impact of cyber security in geopolitics. Journal of Geographical Research No. 30, 239-260.
9- Ziyad Ali Al- Ali. (2019). Conflict and geocyber security in international politics.

DOI: https://doi.org/10.33193/JEAHS.18.2022.302
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (18) December 2022
العدد (18) ديسمبر 2022

Amman: Dar Amjad for publication and distribution.
10- Salim Dahmani. (2018). The impact of cyber threats on national security, the United States of America as a model. Algeria: Boudiaf University, M'sila.
11- Saleh Mahdi Al-Shammari, Zaid Muhammad Ali Ismail. (2020). Cybersecurity as a new pivot in the Iraqi strategy. Political Issues, Al-Nahrain University, No. 62, 273-296.
12- Ali Fadel Suleiman. (2020). The right to legal defense against cyber attacks. Tikrit: Tikrit University Journal of Law, Issue 4, Volume 4.
13- Fonterre, Daniel. (2019). Cyber strategy, the world of knowledge. Kuwait: National Council for Culture, Arts and Literature.
14- Lubna Khamis Mahdi and Taghreed Safaa. (2020). The impact of cyber on the development of power. Homurabi, 145-161.
15- Marwan Salem Al-Ali. (2020). Strategic challenges to Iraqi national security in light of international changes. Tikrit Journal.
16- Mustafa Ibrahim Salman Al-Shammari. (2021). Cybersecurity and its impact on Iraqi national security. University of Baghdad: Journal of Legal and Political Sciences.
17- Mona Jabbour Ashqar. (2017). Cyber obsession of the age. League of Arab States, Cairo: Arab Center for Legal and Judicial Research.
18- Nasira Salehi. (2021). Smart Power Global competition for cyber power and cyber capabilities. Daftar al-Siyasa wa al-Qanun Volume 13 No. 1, 374-385.
19- Nora Shaloush. (2018). Electronic piracy in cyberspace, the escalating threat to state security. Babel Journal for Human Studies, Issue 2, Volume 8, 199.

.